NORTEL NETWORKS

Enterprise Edge 2.0 Programming Operations Guide

1-800-4 NORTEL
www.nortelnetworks.com

© 2000 Nortel Networks
P0911588 Issue 01

Contents

Chapter 1 About this document 13

What's new in this document 13
How this guide is organized 13
Related documents 14
Regulations 15
- Safety information for North American customers 15
- Enhanced 911 Configuration 16
- Radio-frequency interference 16
- Telecommunication registration 17
- Hearing-aid compatibility 17
- Electromagnetic compatibility 17
- Telephone company registration 18
- Use of a music source 18
- Rights of the telecommunications company 18
- Repairs 18
- Safety information for European customers 19
- Radio-frequency interference 20

Software licensing 21

Chapter 2 Enterprise Edge Overview 23

Enterprise Edge telephony hardware components 24
Enterprise Edge data networking hardware components 24
Enterprise Edge software components 25
- Enterprise Edge Integrated Solution 25
- Enterprise Edge Voice Messaging 26
- Enterprise Edge Call Center 27
- Enterprise Edge Call Center Reporting 27
- Enterprise Edge Voice over IP gateway 27
- Enterprise Edge TSP 27
- Enterprise Edge Personal Call Manager 27
- Enterprise Edge Call Detail Recording 28
- Enterprise Edge Attendant Consol 28
- Enterprise Edge Integrated QoS Routing 28
- Tivoli 28
- Optivity 28

Unified Manager 28
- Browser requirements 29
- Understanding Unified Manager 30
- Menu descriptions 32
- Enterprise Edge system access 32

Chapter 3 Setting up your Enterprise Edge system 35

Enterprise Edge required parameters 35
Setting up an Enterprise Edge IP Address 36
Setting up web-based administration 37
Browser settings 37
Logging on to Enterprise Edge 37
Preloading Java class files on your workstation 39
Accessing Unified Manager through the Preinstalled Client Home Page 39
Logging off Enterprise Edge 40
Rebooting the Enterprise Edge server 40
Shutting down Enterprise Edge System 40
Licensing 41
Entering the software keycodes 41
Configuring system settings 41
System registration 42
Basic registration using Internet Access 43
Basic Registration using v.90 modem (North America only) 43

Chapter 4 Configuring Enterprise Edge Resources 45

Viewing Enterprise Edge resources 45
LAN 46
Viewing LAN resources and configuring global LAN attributes 46
Configuring LAN resources 46
WAN 49
WAN Overview 49
Permanent WAN Connection 50
Viewing WAN Resources 51
Setting global WAN parameters 51
Configuring WAN Summary Parameters 52
Setting WAN Line Parameters 53
PVC Congestion Control 56
WAN PPP Parameters 57
WAN performance 58
Dial Up 58
Configuring RAS Server TCP/IP 58
ISDN Dial Up 59
V.90 modem (North America) Dial Up 63
Media Services Card 66
Rules for configuring DSP resource allocation 67
DSP Current Configuration 68
DSP Manager 68
DSP Settings 69

Media Bay Modules 69
Bus 71
Module 72
T1 Parameters (North America only) 77
E1 Parameters (Europe) 79
Configuring a data module 79
Provision lines 81

Chapter 5 Configuring Enterprise Edge Services 83

Programming order 83
Programming Services 84
Viewing Enterprise Edge Services 85
Viewing all Services 85
To Enable or Disable a Service 85
Statuses 86
Telephony Services 87
Enhanced 911 (E911) Configuration 89
Terminals & sets 90
Copying settings from one telephone set to another 91
General 91
Line access 93
Capabilities 98
User preferences 102
Restrictions 103
Telco features 106
Lines 108
Copying settings from one line to another 108
General 109
Trunk/line data 111
Setting Received number 117
Restrictions 118
Telco features 120
Loops 121
Restriction filters 124
Time & date 127
Call Routing 128
Routes and destination codes 129
Programming the PRI routing table 130
Destination codes 131
Setting up a route for local calling 133
Setting up a route for long distance calling 134
Adding a long distance carrier access code 135
Programming for least cost routing 136
Using dialing restrictions with routing 137
Using a dialing plan to route outgoing PRI calls 137

Scheduled Services 138
Ringing service 139
Restriction service 141
Routing Service 142
Common Settings 143
System speed dial 145
Adding or changing a system speed dial 145
General Settings 147
Business name 147
Feature settings 148
Call log space 151
Timers 152
Direct dial 153
CAP assignment 154
Dialing plan 154
Access codes 156
Remote access packages 160
COS Passwords 160
DN lengths 162
Network Name Display 163
Programming Network Name Display 165
Call by Call service selection for PRI 166
Programming Call by Call service selection 168
CbC limits 168
Release reasons 169
Network Services 169
Hunt groups 170
Adding or removing members from a group 171
Moving members of a group 172
Assigning or unassigning lines to a group 173
Setting the Distribution mode 174
Setting the hunt delay 174
Companion 177
Registration 177
Changing the Registration password 178
Radio data 179
Register individual portables 181
Portable telephone programming 182
Hospitality 183
Alarm time (AL) feature 184
Set/room settings 185
Call permissions 185
Alarm data 186
Telco features 187
Voice message center numbers 187
Outgoing name and number blocking (ONN) 188

Voice Mail 188
Call Detail Recording 188
TAPI 188
Console Service 189
VoIP Gateway 189
VoIP local and remote gateways 189
DHCP 192
Configuring a DHCPRelayAgent 194
LAN settings for DHCPServer 194
LAN settings for DHCPRelayAgent 198
DNS 199
IP Routing 200
Configuring IP Routing 201
IP Routing global settings 201
Configuring IP routing on an interface 202
IPX Routing 208
Configuring IPX Routing 208
Configuring an interface for IPX routing 209
Adding RIP filters for IPX routing 213
Adding SAP filters for IPX routing 214
Adding Static Routes for IPX Routing 214
Adding Static Service for IPX 215
SNMP 216
SNMP Community List, Manager List, and Trap Community List 217
QoS 220
Relationship between the QoS Module and theVoIP QoS Monitor 220
QoS Restrictions and Defaults 221
Filters 223
QoS performance graphs and tables 225
Port Range Setting for Legacy Networks 225
QoS monitor 227
QoS Monitor Mean Opinion Score 227
Web cache 228
Net Link Manager 229
Selecting the permanent WAN link as the primary WAN connection 230
Selecting a dial-up link as the primary WAN connection 231
Alarm Service 232
NAT (Network Address Translation) 232
Example of a common NAT configuration 235
IP Firewall Filters 235

Chapter 6 Configuring Digital Private Network Signalling System1 241

DPNSS 1 services 241
- DPNSS 1 capabilities 242
- DPNSS 1 features 242

Three Party Service 243
- Making a conference call 243

Diversion 243
- Restrictions by set type 244
- Setting Diversion 245

Redirection 245
- Restrictions by set type 245
- Setting Redirection 245

Executive Intrusion 245
- Restrictions by set type 246
- Intrusion levels 246

Call Offer 247
- Displays 247
- Restrictions by set type 247
- User Actions 248

Route Optimization 248
- Setting Route Optimization 248

Message Waiting Indication 249
- Restrictions by set type 249
- Setting Message Waiting Indication 249

Loop avoidance 252
- Programming Loop avoidance 252

Chapter 7 Configuring Management Settings 253

User Manager 253
- Adding a user profile 254
- Modifying a user profile 254
- Deleting a user profile 255

Alarm Manager 256
- Configuring the Alarm Manager 256

Chapter 8 Maintenance 259

Enterprise Edge general maintenance 259
- System startup 259
- Warm reset 260
- Backup and restore 260
- Backup, restore, upgrade utility (BRU) for Enterprise Edge system 261
- Backup and restore telephony programming using Unified Manager's Tools menu 265

Enterprise Edge system diagnostics and utilities 269
Performance Statistics 269
Error Messages 270
MIB II Information 274
Maintenance programming for telephony resources 278
System version 278
Media Bay Module status 279
System test log 282
System administration log 283
Network event log 284
Alarm codes 285
Event messages 285
Tests 294
CSU statistics 297
Link Status 301
Metrics 301
Moving telephones 302

Chapter 9 Troubleshooting your Enterprise Edge system 305

General troubleshooting information 305
Getting ready 306
Types of problems 306
Basic troubleshooting procedure 306
Viewing system performance and fault alarms 307
System performance graphs and tables 308
Fault Alarm Banner 308
Problems with telephones 309
Telephone has faulty buttons, display, handset or other hardware problems 309
Digital telephone display is unreadable 309
Telephone has no dial tone 310
Problems with lines 310
Calls can be received but cannot be made 310
Dial tone is absent on external lines 311
Lines at a telephone are busy after call is over 311
Auto-answer line rings at a telephone 313
Prime telephone gets misdialed calls 314
Selected lines reads “Not in service” or “Not available” 314
Selected line pool shows “No free lines” 315
Problems with optional equipment 315
Problems with the Enterprise Edge ATA 2 316
Problems with the auxiliary ringer 316
Problems with external paging 317
Problems with Music on Hold and Background Music 317

Problems with module service 318
Digital Trunk Computer Module trouble 318
Monitoring the T1 or PRI signal 320
Problems with Trunk or Station Modules 320
Problems for network or remote users 321
Remote feature code gets no response 321
Dialed number gets ringback and the wrong person 322
Dialed number gets dial tone instead of ringback 322
Dialed number gets busy tone 322
Dialed number does not get through 322
Dialed feature code gets overflow tone 323
Dialed feature code gets busy tone 324
Line pool access code gets overflow tone 324
Line pool access code gets ringback 325
Line pool access code gets busy tone 325
Dialed number gets no response 325
Problems with Companion sets (North American systems only) 326

Appendix A: Network Examples 327

Access using Enterprise Edge 328
Lines used for networking 328
PRI lines 329
T1 lines (Loop, E&M, DID, Ground start) 329
BRI lines 330
DPNSS lines (International systems only) 330
Remote system access to Enterprise Edge 330
Remote access on loop start trunks 331
Remote access on a private network 331
Remote access on T1 Direct Inward Dial (DID) trunks 332
Remote access on PRI trunks 332
Remote access on DPNSS lines 332
Enterprise Edge security 333
Class of Service 333
Restriction filters 333
Direct inward system access (DISA) 335
Coordinated dialing plans 335
Dialing plan using public lines 335
Dialing plan using T1 E&M lines 337
Dialing plans with shared line pools 340
Networking examples 341
PRI Networking with Meridian 1 341
PRI networking using Call-by-Call Services 346
Enterprise Edge VoIP Gateway and M1 networking 348
Toll bypass with Enterprise Edge VoIP Gateway 351
Networking with QSIG (International systems only) 356

Private networking with DPNSS (International systems only) 359
Public networking scenarios 362
Call one or more Enterprise Edge telephones 363
Call Enterprise Edge and select tie lines to a private network 363
Call Enterprise Edge and select lines to the public network 364
Private networking scenarios 365
Call one or more Enterprise Edge telephones 366
Call Enterprise Edge and select tie lines to other nodes in the private network 366
Call Enterprise Edge and select lines to the public network 367
Select T1 E&M trunks to the private network 368
Using Enterprise Edge Line Redirection 368
PRI dialing plan example for 2-way DID 370
PRI DID and 2-way DID 370

Appendix B: ISDN Overview 371

Welcome to ISDN 371
Analog versus ISDN 371
Types of ISDN service 372
ISDN layers 372
ISDN Bearer capability 373
Services and features for ISDN BRI and PRI 373
PRI services and features 373
BRI services and features 373
ISDN hardware 377
PRI hardware 377
BRI hardware 378
Clock Source for ISDN 379
Other ISDN BRI equipment 380
ISDN standards compatibility 380
Planning your ISDN network 380
Ordering ISDN PRI 381
Ordering ISDN BRI 381
Supported ISDN protocols 382
ISDN programming 383
Program ISDN equipment 386

Appendix C: Setting Up Remote Routers 389

Creating an Outbound Traffic Filter 389
Sample Criteria, Ranges, and Actions for UDP Filtering 390

Appendix D: Market profile attributes 391

Languages available to customer 391
System defaults 392

Glossary 395

Index 437

About this document 1

This guide explains how to program your Enterprise Edge system. For more information about the Enterprise Edge document suite, refer to Related documents on page 14.

Note: The section Regulations on page 15 summarizes the Enterprise Edge system regulatory information.

The section Software licensing on page 21 contains software licensing information.

What's new in this document

This release includes additional information regarding:

- market profile attributes for United Kingdom markets
- updated backup and restore procedures for the BRU utility
- automatic registration of Enterprise Edge with the Tivoli Management Server
- Optivity interworking in the areas of network discovery, SNMP alarms integration, and launching of the Unified Manager
- DSP allocation through the DSP Manager
- IPX routing configuration for networking
- primary and backup dialup WAN connections using ISDN or V.90 modem (The V.90 modem is available in North America only.)
- OSPF routing protocol
- firewall filters
- network address translation (NAT)

How this guide is organized

This document contains the following sections:

- Enterprise Edge Overview on page 23 provides an overview of the hardware and software components of the Enterprise Edge system and a description of Unified Manager.
- Setting up your Enterprise Edge system on page 35 includes information on how to set up your IP address and Web-based administration, how to configure your system settings and other basic procedures such as logging on and off your Enterprise Edge system.

- Configuring Digital Private Network Signalling System1 on page 241 describes the procedures used to program the Digital Private Network Signalling System (DPNSS 1) for International systems only.
- Configuring Enterprise Edge Resources on page 45 describes the procedures used to program the networking resources for your Enterprise Edge system.
- Configuring Enterprise Edge Services on page 83 describes the procedures used to program all the Enterprise Edge services.
- Configuring Management Settings on page 253 includes procedures used to program user and alarm settings.
- Maintenance on page 259 includes all the maintenance procedures required to keep your system in operation. This chapter ncludes descriptions of how to perform both a system and telephony programming backup and restore.
- Troubleshooting your Enterprise Edge system on page 305 allows you to solve problems in the Enterprise Edge system that require changes to system programming.
- Appendix A: Network Examples on page 327 includes some networking examples using the Enterprise Edge system.
- Appendix B: ISDN Overview on page 371 includes some background information about ISDN.
- Appendix C: Setting Up Remote Routers on page 389 explains how to set up a Nortel Networks (BayRS) router.
- Appendix D: Market profile attributes on page 391 describes the functionality associated with each of the Enterprise Edge market profiles.
- Glossary on page 395 contains a list of Enterprise Edge terms and definitions.

Related documents

In addition to the *Enterprise Edge Programming Operations Guide*, the Enterprise Edge documentation suite contains the following documents:

- *Enterprise Edge Feature Programming Telephone Guide*
- *Enterprise Edge 2.0 Installation and Maintenance Guide*
- *Enterprise Edge IP Telephony Configuration Guide*
- *Enterprise Edge 2.0 Voice Messaging Set Up and Operation Guide*
- *Enterprise Edge 2.0 Voice Messaging Reference Guide*
- *Enterprise Edge 2.0 Voice Messaging Quick Reference Guide*
- *Enterprise Edge 2.0 Voice Messaging Programming Record*
- *Enterprise Edge 2.0 Voice Messaging AMIS Set Up and Operation Guide*
- *Enterprise Edge 2.0 Voice Messaging AMIS User Guide*
- *Enterprise Edge **2.0** Unified Messaging Client Installation Guide*

- *Enterprise Edge 2.0 Unified Messaging Quick Reference Guide*
- *Enterprise Edge Software Keycode Installation Guide*
- *Enterprise Edge 2.0 Call Center Set Up and Operation Guide*
- *Enterprise Edge 2.0 Call Center Agent Cards*
- *Enterprise Edge 2.0 Call Center Reporting Set Up and Operation Guide*
- *Enterprise Edge 2.0 TSP Server Configuration Guide*
- *Enterprise Edge 2.0 Personal Call Manager User Guide*
- *Enterprise Edge 2.0 Attendant Console Set Up and Operation Guide*
- *Enterprise Edge 2.0 Attendant Console User Guide*
- *Enterprise Edge 2.0 Call Detail Recording System Administrator Manual*
- *Enterprise Edge 2.0 ATA 2 Installation Guide*
- *Enterprise Edge 2.0 ATA 2 User Guide*
- *Enterprise Edge 2.0 Message Networking Set Up and Operation Guide*
- *Enterprise Edge 2.0 Message Networking User Guide*
- *Enterprise Edge 2.0 Fax Set Up and Operation Guide*
- *Enterprise Edge 2.0 Fax User Guide*

You can also access a number of telephone and accessory quick reference cards.

Regulations

Safety information for North American customers

Enterprise Edge equipment meets all applicable requirements of both the CSA C22.2 No. 950-95 and UL-1950 Edition 3.

Risk of shock.
Do not plug in the computer or any telephone or network cables before opening the computer.

Read and follow installation instructions carefully.

Only qualified persons can service the system.

The installation and service of this hardware is hazardous and can cause severe harm to the person performing the tasks or to other persons. Only qualified service personnel must perform the installation and service tasks.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to themselves and users, the service personnel must connect the Enterprise Edge system to an outlet equipped with a third-wire ground.

Service personnel must be alert to the risk of high leakage currents spreading onto metal system surfaces during power line fault events near network lines. These leakage currents flow to Protective Earth ground through the power cord. Because of the protective function of earth ground, when cabling the unit, the first task the service personnel must perform is the connection to an earthed outlet.. Subsequently, the last task to perform is the removal of the the connection. It is important that operations requiring the unit to be powered down must have the network connections (central office lines) removed first.

Enhanced 911 Configuration

Warning

Local, state and federal requirements for Emergency 911 services support by Customer Premises Equipment vary. Consult your telecommunication service provider regarding compliance with applicable laws and regulations.

Note: For information about 911 configuration, refer to Enhanced 911 (E911) Configuration on page 89.

Radio-frequency interference

Equipment generates RF energy.

This equipment generates, uses, and can radiate radio-frequency energy. If not installed and used in accordance with the installation manual, it may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Part 15 of the FCC Rules and with ICES.003, CLASS A Canadian EMI Requirements. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Telecommunication registration

Enterprise Edge equipment meets all applicable requirements of both Industry Canada CS-03 and US Federal Commission FCC Par t68 and has been registered under files Industry Canada 332-5980 A and
FCC AB6CAN-20705-KF-E (key system), AB6CAN-20706-MF-E (hybrid system), and AB6CAN-23740-PF-E (PBX system). Connection of the Enterprise Edge telephone system to the nationwide telecommunications network is made through a standard network interface jack that you can order from your local telecommunications company. This type of customer-provided equipment cannot be used on party lines or coin lines.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Only qualified persons can service the system.

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician.

Hearing-aid compatibility

Enterprise Edge telephones are hearing-aid compatible, as defined in Section 68.316 of Part 68 FCC Rules.

Electromagnetic compatibility

Enterprise Edge equipment meets all FCC Part 15, Class A radiated and conducted emissions requirements.

Enterprise Edge does not exceed the Class A limits for radiated and conducted emissions from digital apparatus as set out in the Radio Interference Regulations of Industry Canada.

Telephone company registration

It is usually not necessary to call the telecommunications company with information on the equipment before connecting the Enterprise Edge system to the telephone network. If the telecommunications company requires this information, provide the following:

- telephone number(s) to which the system will be connected
- FCC registration number (on label affixed to Enterprise Edge)
- universal service order code (USOC)
- service order code (SOC)
- facility interface code (FIC)

Use of a music source

In accordance with U.S. Copyright Law, a license may be required from the American Society of Composers, Authors and Publishers, or similar organization if Radio or TV broadcasts are transmitted through the Music On Hold or Background Music features of this telecommunication system.

Nortel Networks hereby disclaims any liability arising out of the failure to obtain such a license.

Rights of the telecommunications company

If the Enterprise Edge system is causing harm to the telephone network, the telecommunications company may discontinue service temporarily. If possible, the telecommunications company will notify you in advance. If advance notice is not practical, the user will be notified as soon as possible. The user will be given the opportunity to correct the situation and informed of the right to file a complaint to the FCC.

The telecommunications company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of the system. If this happens, the telecommunications company will give you advance notice in order for you to make any necessary modifications to maintain uninterrupted service.

Repairs

In the event of equipment malfunction, all repairs to certified equipment will be performed by an authorized supplier.

Safety information for European customers

WARNING
The instructions in this manual are intended to be performed by Qualified Service Personnel.

The CE mark indicates that the Enterprise Edge equipment meets the requirements of the following EU Directives:

- Low Voltage Directive (73/23IIC)
- Electromagnetic Directive (89/336/EEC)

Risk of shock.
Ensure the computer is unplugged from the power socket and that any telephone or network cables are unplugged before opening the computer.

Read and follow installation instructions carefully.

Only qualified persons should service the system.
The installation and service of this hardware is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the Enterprise Edge system must be connected to an outlet with a third-wire Earth.

Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (exchange lines) removed first.

Radio-frequency interference

WARNING

This is a Class A product. In a domestic environment this product may cause interference. The user may be required to take adequate measures.

Read and follow installation instructions carefully

This product uses Telecommunication Network Voltage (TNV) circuits which include the following ports: analogue lines (including PFT), modems, ATA, BRI, AC15A, and TCM Isolator.

This product uses Safety Extra Low Voltage (SELV) circuits which include the following ports: TCM extensions, external music source (MSCX), auxiliary ringer (AUX), paging system relay (PAGE), LAN interface, WAN interface, and the serial port.

Software licensing

Copyright (c) 1995-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

> “This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

> For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called “Apache” nor may “Apache” appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).”

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see http://www.apache.org/.

Enterprise Edge Overview 2

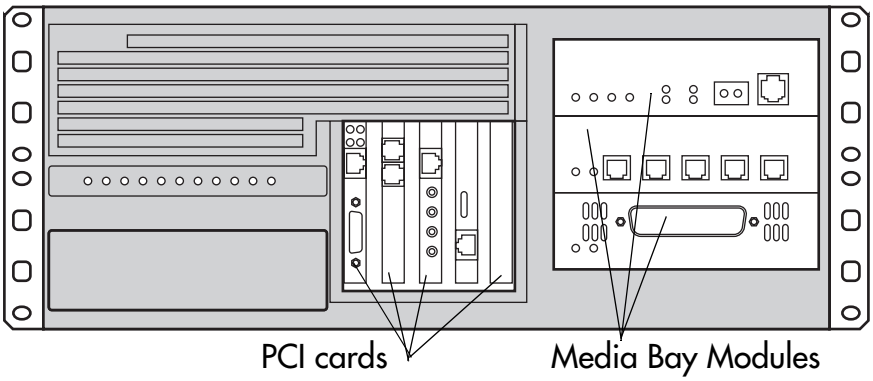
The Enterprise Edge system includes software and hardware components that provide telephony technology, basic voice messaging, data networking and IP telephony.

The Web-based navigation tool Unified Manager provides easy access to all Operations and Maintenance programming on the Enterprise Edge system at a single site. For more information about Unified Manager, see page 28.

Tivoli provides multi-site and multi-network system management. For more information, refer to Tivoli on page 28. Optivity provides multi-site network management. For more information, refer to Optivity on page 28.

Note: Some of the components described in this section are not available in all areas. Ask your Nortel Networks Enterprise Edge supplier for information about the availability of components.

The main component of the Enterprise Edge system is the Enterprise Edge server. The Enterprise Edge server controls all tasks such as call processing, voice messaging, and data routing. The Enterprise Edge server also contains the telephony and data networking components.



The system components are summarized in:

- Enterprise Edge telephony hardware components on page 24
- Enterprise Edge data networking hardware components on page 24
- Enterprise Edge software components on page 25

For a detailed description of each hardware components, refer to the *Enterprise Edge Installation and Maintenance Manual*.

Enterprise Edge telephony hardware components

The telephony components perform call processing. These components also connect the Enterprise Edge server to the Public Switched Telephone Network (PSTN) lines and the Enterprise Edge telephones. The telephony hardware components of the Enterprise Edge system include:

- Media Services Card (MSC), which is a PCI standard card that perform call processing and media processing of the voice channels.
- Station set Media Bay Modules, which provide access to telephone lines. The Enterprise Edge system includes the following station set media bay modules:

  - 16-port Digital Station Media Bay Module (EE-DSM 16), which allows the connection of 16 digital telephone sets to the system

  - 32-port Digital Station Media Bay Module (EE-DSM 32), which allows the connection of 32 digital telephone sets to the system

  - Analog Station Media Bay Module (EE-ASM 8), which allows the connection of analog station sets to the system (**North American systems only**)
- Trunk Media Bay Modules, which provide access to telecommunications trunks. The Enterprise Edge system includes the following trunk media bay modules:

  - Digital Trunk Media Bay Module (EE-DTM), which provides the connection between a standard digital PSTN T1 or PRI line and the Enterprise Edge system.

  - Caller ID Trunk Media Bay Module (EE-CTM), which provides the ability to access four analog Caller ID PSTN lines. (**North American systems only**)

  - Basic Rate Interface Media Bay Module (EE-BRIM S/T), which provides the ability to access up to four BRI S/T ISDN lines.

  - Fibre Expansion Media Bay Module (EE-FEM), which provides the ability to access up to six Norstar expansion modules. These expansion modules add PSTN lines and telephones to the Enterprise Edge system.
- Station sets and adapters

Enterprise Edge data networking hardware components

The data networking components connect the Enterprise Edge server to the local area network (LAN) and the wide area network (WAN). The data networking hardware components of the Enterprise Edge system include:

- V.90 modem card used to send and receive data using the public telephone system. (**North American systems only**)
- LAN interface card to connect the Enterprise Edge system to the local area network. This card is a 10/100 Base T Ethernet network interface card.
- WAN interface card to connect the Enterprise Edge system to the wide area network. North American systems have a T1 interface port and a synchronous port. European systems have two serial synchronous ports.

Enterprise Edge software components

The Enterprise Edge system provides a number of software applications. Some of these applications work immediately after you install the Enterprise Edge system. To use other applications, you must enable the application using software keycodes. A software keycode is a password number provided to the installer. The Enterprise Edge applications available are:

- Enterprise Edge Integrated Solution on page 25
- Enterprise Edge Voice Messaging on page 26
- Enterprise Edge Call Center on page 27
- Enterprise Edge Call Center Reporting on page 27
- Enterprise Edge Voice over IP gateway on page 27
- Enterprise Edge TSP on page 27
- Enterprise Edge Personal Call Manager on page 27
- Enterprise Edge Call Detail Recording on page 28
- Enterprise Edge Attendant Consol on page 28
- Enterprise Edge Integrated QoS Routing on page 28

For information on enabling software applications, refer to the *Enterprise Edge Software Keycode Installation Guide*.

Enterprise Edge Integrated Solution

Enterprise Edge Integrated Solution software supplies standard telephony operating features plus the following additional features:

- Enterprise Edge Companion (North American systems only) on page 25
- Programming, administration and maintenance on page 25

Enterprise Edge Companion (North American systems only)

The Enterprise Edge Companion Wireless software provides wireless functionality without losing the advantages of the wired system.The system can be programmed so that users can publish one telephone number and receive all calls on both their desk set and their portable, allowing them to answer the one who is most convenient.

Programming, administration and maintenance

The Enterprise Edge Unified Manager software provides programming, administration and maintenance. Enterprise Edge Unified Manager provides a series of windows and menus which allow you to navigate through the different areas of the application and program the system. For more information on Unified Manager, refer to Unified Manager on page 28.

Enterprise Edge Voice Messaging

Enterprise Edge Voice Messaging is a Windows™ based application that allows the user to set up and administer the following Voice Messaging features:

- Voice messaging on page 26
- Enterprise Edge Auto attendant on page 26
- Custom Call Routing (CCR) on page 26
- Enterprise Edge Networking on page 26
- Enterprise Edge Unified Messaging on page 26

Voice messaging

Voice messaging records caller's messages and stores them in a mailbox for easy retrieval. Each Enterprise Edge telephone in your system can have its mailbox and personal greeting.

Enterprise Edge Auto attendant

Auto attendant answers business calls with a Company Greeting. A voice prompt then offers callers a menu of options to direct their call by selecting a digit on the dial pad.

Custom Call Routing (CCR)

CCR replaces the Automated Attendant menu with a customized CCR Home Menu to offer callers a wider range of call routing options and access to submenus and information messages. CCR allows you to determine the menu options and record the voice prompts that guide callers along call paths.

Enterprise Edge Networking

Enterprise Edge Networking includes General Networking parameters, Voice Profile for Internet Mail (VPIM) parameters, Audio Messaging Interchange Specification (AMIS) specific parameters and AMIS Site Administration. For more information about Enterprise Edge Networking, refer to the *Enterprise Edge Networking Set Up and Operation Guide*.

Enterprise Edge Unified Messaging

Enterprise Edge Unified Messaging includes three features:

- **Enterprise Edge Unified Messaging** allows you to create and receive messages on your personal computer.
- **Enterprise Edge Personal Mailbox Manager** allows you to change mailbox features and functions such as mailbox initialization and target attendant, record greetings, and set up and maintain off-premise message notification.
- **Enterprise Edge Operator Manager** allows you to change the Operator password, change business status, enable or disable the system attendant and enable or disable the Call Answer feature.

For more information, refer to the *Enterprise Edge Unified Messaging Client Installation Guide.*

Enterprise Edge Call Center

The Enterprise Edge Call Center is an Automatic Call Distribution (ACD) system designed to handle incoming calls. Incoming calls are distributed to available agents or to Enterprise Edge greetings in your call center. To ensure that each call is handled correctly, the Enterprise Edge Call Center system answers, plays greetings and routes each incoming call to the first available agent in the order of the call's arrival. For more information, refer to the *Enterprise Edge Call Center Set Up and Operation Guide*.

Enterprise Edge Call Center Reporting

Enterprise Edge Call Center Reporting is a Windows software application that provides Real Time statistics and complete management information on the daily performance of your Enterprise Edge system. Enterprise Edge Call Center Reporting helps you manage call traffic and provides a full range of management reports that provides critical information for accurate business planning. It also has the ability to support multiple Wallboards which can be configured separately to display the information that the agents require. For more information, refer to the *Enterprise Edge Call Center Reporting Set Up and Operation Guide*.

Enterprise Edge Voice over IP gateway

Enterprise Edge VoIP Gateway allows you to use IP telephony. VoIP Gateway converts the voice in a call into a packet format that can be sent over an intranet. With Enterprise Edge VoIP Gateway, you can make telephone calls over any intranet connected to the Enterprise Edge system. For more information, refer to the *Enterprise Edge IP Telephony Configuration Guide*.

Enterprise Edge TSP

Enterprise Edge TSP is the interface between the Enterprise Edge system and Microsoft®[1] TAPI. This interface allows you to use TAPI applications on the Enterprise Edge system. For more information, refer to the *Enterprise Edge TSP Server Configuration Guide*.

Enterprise Edge Personal Call Manager

Enterprise Edge Personal Call Manager is a TAPI application that allows you to control your Enterprise Edge telephone from your personal computer. For more information, refer to the *Enterprise Edge Personal Call Manager User Guide*.

1.Microsoft is a registered trademark of Microsoft Corporation.

Enterprise Edge Call Detail Recording

The Enterprise Edge Call Detail Recording software records call activity. When a telephone call is made to or from your company, the information about the call is recorded. When the call is completed, information about the call is printed out in Call Records. For more information, refer to the *Enterprise Edge Call Detail Recording System Administrator Guide*.

Enterprise Edge Attendant Consol

Enterprise Edge Attendant Console uses a graphical user interface to provide centralized call management. For more information, refer to the *Enterprise Edge Attendant Console Set Up and Operation Guide* and the *Enterprise Edge Attendant Console User Guide*.

Enterprise Edge Integrated QoS Routing

Enterprise Edge Integrated QoS Routing controls the interface between the Enterprise Edge system and the local area network, wide area network, and Internet.

Tivoli

Tivoli provides inventory management, multi-site software distribution and service level and status monitoring. All Enterprise Edge systems are sold with an imbedded Tivoli Management Agent (TMA) that allows Enterprise Edge to connect to a central server where the software resides. When installed, all Enterprise Edge systems automatically register with the central TMR server. For more information, refer to System registration on page 42.

Optivity

Optivity allows the customer to view the topology of the network including the Enterprise Edge, other routers, hubs, switches and servers and see how the different devices are connected and performing. The Optivity management station can be used to capture SNMP alarms sent from Enterprise Edge. Unified Manager can be launched from within the Optivity Management Tool suite. For more information, refer to the Optivity documentation

Unified Manager

The Enterprise Edge Unified Manager provides a web-based navigation tool that lets you view and change configuration for:

- system settings
- IP Services
- VoIP Service
- Telephony Services
- Management Server Module

- QoS Module
- Diagnostics

Most changes made with Unified Manager become part of current Enterprise Edge programming when you select an item from the menu options. However, some changes take effect a minute after the user stops programming. If a programming error occurs, you must reenter the original programming.

For more information on Unified Manager, refer to

- Browser requirements on page 29
- Understanding Unified Manager on page 30
- Enterprise Edge system access on page 32

Browser requirements

Your computer must meet the following requirements to configure Enterprise Edge through the Unified Manager.

- WinNT or Windows workstation running on P133 or higher CPU (or compatible)
- 64 MB RAM, 10 MB disk space
- Minimum screen definition of 1024 X 768
- Minimum monitor size of 17 inches

To use Enterprise Edge Unified Manager, you must have:

- Java Virtual Machine (JVM) 5.0 (build 5.0.0.3188 or greater)
- One of the following web browsers:

  Netscape Communicator 4.5 or greater
  Microsoft Internet Explorer 4.0 or greater

If you are using Netscape Communicator, you must set the following parameters:

- Enable Java: On
- Cached document comparison: Every time

If you are using Microsoft Internet Explorer, you must set the following parameters:

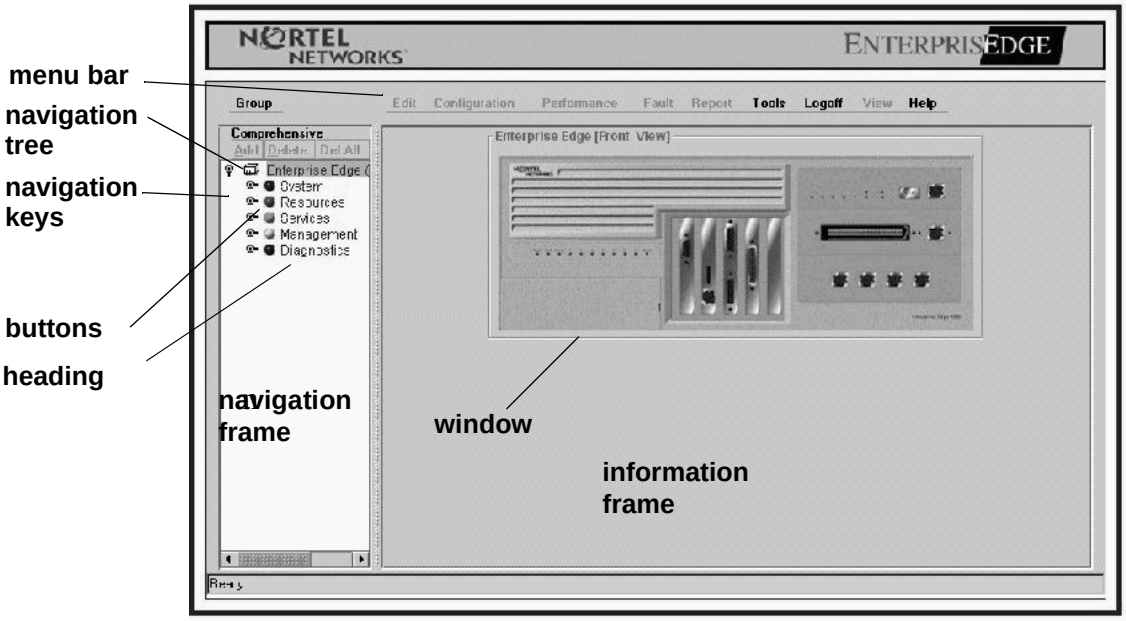
- Check for newer versions: Every visit to the page
- Java JIT compiler enabled: On

For information about setting these parameters, refer to the user documentation that came with your web browser.

Understanding Unified Manager

Unified Manager consists of:

- a menu bar where users access configuration commands
- a navigation frame where is located the navigation tree that allows you to navigate through Enterprise Edge programming headings
- an information frame that displays the windows that relates to the headings you select in the navigation frame



The menu bar contains configuration management options. These options are enabled when you select the different headings in the navigation tree to enter specific areas of the Enterprise Edge system. If an option is dimmed, it is not available for the heading you have selected.

The navigation tree contains headings that allow you to access specific areas of the Enterprise Edge system. The key symbol ( ) beside each heading indicates that the heading can be expanded to show sub-headings. To make sub-headings appear, double-click the item or just click on the key itself. As you select various headings in the navigation tree, the heading changes color and Unified Manager displays the appropriate information frame.

The information frame can contain configuration windows or dialog boxes indicating the appropriate action and system messages or warnings.

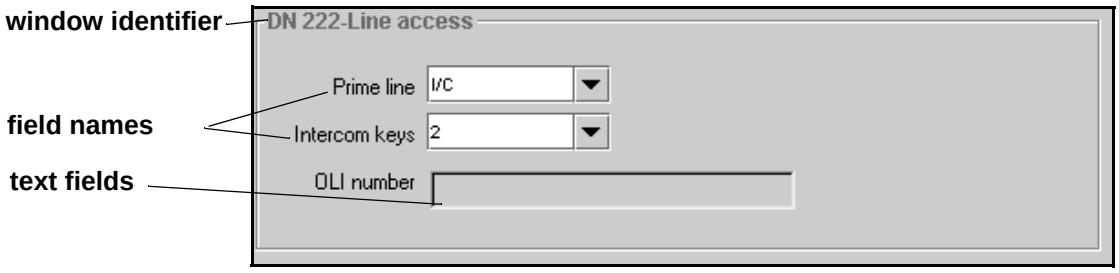
For more detailed information on Unified Manager, refer to:

- Using the configuration windows on page 31
- Changing data views in Unified Manager on page 31

Using the configuration windows

The configuration windows are used to configure Enterprise Edge settings. The configuration windows always contain a window identifier. Some fields use edit-in-place formats to allow you to configure settings in the box opposite each box name. When you tab to the next box, the previous box values are saved. Some box use drop-down list to provide you with valid entries.

If a value is invalid, an error message appears to alert you of the error. The dialog box format allows you to enter text in boxes and save the settings by clicking the **Save** button where available or by simply moving to another heading in the navigation tree.



Changing data views in Unified Manager

You can change the order and size of data views in the Unified Manager.

Use the following procedure to change the column order.

1. Point to the column that you want to move and click on it.

2. Holding the mouse down, drag and drop the column to the appropriate location.

   The other column in this location, automatically changes places with the column you are moving.

Use the following procedure to change the column width of any column in the display.

1. Keeping the pointer in the heading row, move it over any column edge until it changes to a double-headed arrow.

2. Drag the column edge to the appropriate location.

Menu descriptions

You access Enterprise Edge functions using the menu. The menu is dynamic which means that the menu commands change depending on the heading you select from the navigation tree.

Menu descriptions

Use	To
Group	View the system, resources, services, and management.
Edit	Edit parameters.
Configuration	Access configuration dialog boxes and screens.
Performance	Access performance graphs and tables.
Fault	Access fault management settings.
Report	Generate a report.
Tools	Use Enterprise Edge tools.
Logoff	Log off, reboot or shutdown the Enterprise Edge server.
View	Refresh the information window to reflect configuration changes.
Help	Access online help.

Enterprise Edge system access

Note: System access must be controlled by providing one userid, the administrator, with read-write privileges. All other users must be given read-only privileges. This prevents concurrent configuration of the Enterprise Edge system. For information on defining user profile and password, see User Manager on page 253

The Unified Manager's navigation tree contains five main headings that allow you to access specific areas of the Enterprise Edge system. The main headings are:

- System on page 32
- Resources on page 33
- Services on page 33
- Management on page 33
- Diagnostics on page 33

System

When you select the **System** heading, you can view system information such as your system name and description and which resources and services are available. When you select the **System** heading, the following menu options are enabled: **Configuration**, **Performance**, **Fault**, **Logoff**, **View** and **Help**. These menu options provide access to statistical information, allow you to enable or disable services and perform system reboot or shutdown. For more information on configuring your system settings, refer to the Configuring system settings on page 41. For information on Performance and Fault monitoring, refer to Viewing system performance and fault alarms on page 307 and Enterprise Edge system diagnostics and utilities on page 269.

You can expand the navigation tree under the **System** heading to find the **Licensing** and the **Identification** subheadings.

Resources

The subheadings under the **Resources** heading, allow you to configure the following resources:

- LAN
- WAN
- Media Services Card
- Media Bay Modules
- Dial Up

For more information on resource programming, refer to Configuring Enterprise Edge Resources on page 45.

Services

Use the options under the **Services** heading to configure services for the Enterprise Edge system, including telephony services. For more information on configuring these settings, refer to Configuring Enterprise Edge Services on page 83.

Management

Use the options under the **Management** heading to configure network management parameters for User Manager and Alarm Manager. For more information, refer to Configuring Management Settings on page 253.

Diagnostics

Use the options under the **Diagnostics** heading to generate and access statistics on different system components. Enterprise Edge provides various statistics, metrics and event logs on resources and services to help you carry out system maintenance activities. For more information on using diagnostics tools, refer to Maintenance on page 259.

Setting up your Enterprise Edge system 3

Refer to the following information when setting up your Enterprise Edge system.

- Enterprise Edge required parameters on page 35
- Setting up an Enterprise Edge IP Address on page 36
- Setting up web-based administration on page 37
- Logging on to Enterprise Edge on page 37
- Logging off Enterprise Edge on page 40
- Rebooting the Enterprise Edge server on page 40
- Shutting down Enterprise Edge System on page 40
- Licensing on page 41
- Configuring system settings on page 41
- System registration on page 42

Enterprise Edge required parameters

The Enterprise Edge quick start module provides quick access to the parameters necessary for the Enterprise Edge server to become active online. However, you must enter a minimum set of parameters within the quick start module. For more information, see the *Enterprise Edge Installation and Maintenance Guide*.

Obtain the required parameter values from an Internet Service Provider (ISP) or corporate network administrator.

Note: Configure all the required parameters during the initial configuration session after you power on the Enterprise Edge server and connect with either an RS-232 or an Ethernet port. After you configure the parameters, reboot the Enterprise Edge server from either the console or Unified Manager.

Enterprise Edge required parameters are:

- Initial IP address and mask for each network interface
- Primary (and optional secondary) DNS servers
- Default next-hop router
- Fractional T1 channel numbers (if you are using fractional TI)
- System name
- WAN link protocol
- Frame Relay DLCI / CIR (if applicable)

- V.90 modem dial-up username and password (North America only)
- V.90 modem dial-up phone number and optional alternate phone number (North America only)

The following table describes the Enterprise Edge server connectivity options.

Field	Definition
HTTP	You can connect to Enterprise Edge from your PC using your JAVA-enabled Internet browser.
TTY	You can connect a dumb terminal to the console of the Enterprise Edge server through an RS-232 cross-over cable, or you can use Hyperterminal from Win95/ Win NT systems. Refer to the appropriate installation guide for information on how to use the console menus.

Setting up an Enterprise Edge IP Address

To manage the Enterprise Edge server using a web browser or an RS-232 connection, you must first set up the IP address. The Enterprise Edge server LAN interface is shipped with default IP address 10.10.10.1 and mask 255.255.255.0. You can change the Enterprise Edge IP address using

To set up the Enterprise Edge server initial IP address using a RS-232 port:

1. Plug in the Enterprise Edge server.
2. Connect a PC or laptop computer to the Enterprise Edge server RS-232 port using a null modem cable.
3. Start a HyperTerminal session on the PC or laptop computer.
4. Enter the LAN/WAN IP address and all other required parameters.

To set up the Enterprise Edge server IP address using a LAN:

1. Plug in the Enterprise Edge server.
2. Connect a laptop to the Enterprise Edge server by Ethernet (back-to-back by using a crossover cable to avoid disturbing the corporate LAN).
3. Set your PC or laptop computer IP address to 10.10.10.2 with a mask 255.255.255.0.
4. Start a web browser on your laptop with a URL of 10.10.10.1.

Setting up web-based administration

You can establish web-based administration to manage the Enterprise Edge system using Unified Manager. Your PC must be set up as an Enterprise Edge client with Internet Explorer 4.0 or greater and a JAVA Virtual Machine (JVM) 5.0.0.3188 or greater installed.

To install JVM on a workstation, search the Microsoft information web page for instructions.

For information on minimum computer or software requirements refer to the *Enterprise Edge Installation and Maintenance Guide*.

Note: The ideal display setting for a monitor attached to Enterprise Edge is 1280 x 1024.

Browser settings

Set your browser as follows:

Program	Required Settings
Netscape Communicator 4.5 or greater	Enable Java: On Category: Cache Cached document comparison: Every Time
Internet Explorer 4.0 or greater	Check for newer versions of stored pages: Every visit to the page Advanced Java VM Java JIT compiler enabled

Unified Manager allows multiple users to log on to the Enterprise Edge system. If more than one user log on to configure the same or related subsystems, the most recent modification remains in effect and overwrites changes previously made.

Maintain one user profile with system administrator privileges. If you have more than one system administrators, you must plan configuration changes carefully. For information on managing user profile and system access, see User Manager.

Note: When configuring Enterprise Edge using Unified Manager, you must disable proxies and directly access Enterprise Edge. The procedure to disable proxies depends on the browser and version.

Logging on to Enterprise Edge

You can access the Enterprise Edge system from another computer through a WAN/Internet connection or a dialup connection. The dialup connection uses either the built in V.90 modem (North America only) or an ISDN dialup. Either access method creates an IP connection that enables all IP-based management tools. For more information on remote connections, refer to Dial Up on page 58.

Use the following procedure to log on to Enterprise Edge using the web browser:

1. Launch your web browser.

2. In the URL address field, type the Enterprise Edge IP address and add port 6800.
   For example: HTTP://10.10.10.1:6800
   The Enterprise Edge Unified Manager initial page is displayed.

3. Click the **Configure** button.
   The Enterprise Edge login screen appears.

4. In the **Login** box, type your login name.
   The default login name is *supervisor*.

5. In the **Password** box, type your password.
   The default password is *visor*.

Tips
Make sure to change the password after you first log on to Enterprise Edge. For information on how to change passwords and to define user profiles, see User Manager on page 253.

6. Click the **Connect** button.
   The Enterprise Edge Unified Manager software starts. Depending on your system, Unified Manager software can take up to several minutes to initialize.

Tips
Performance at startup of Unified Manager is enhanced by preloading the Java class files on all PCs and laptops from which you want to access Enterprise Edge using Unified Manager. Prelaoding the Java class files on your workstation saves time because the Enterprise Edge server does not need to download Java class files to your PC when you launch Unified Manager. See Preloading Java class files on your workstation.

The login screen includes:

Field	Definition
Login	Allows you to enter the user name. The name can contain up to 50 case-sensitive alphanumeric characters. The default log in name for a system administrator is *supervisor*.
Password	The Enterprise Edge password associated with the login name. The password can contain up to 12 case-sensitive alphanumeric characters. The default system administrator password is *visor*.
Configure	Allows you access Enterprise Edge configuration.

Preloading Java class files on your workstation

To preload Java class files on your workstation:

1. From your PC **Start** menu, choose **Find** and then **Computer...**

2. In the **Named:** box, enter your Enterprise Edge system name.

Tips
If you do not know your Enterprise Edge system name, log on to Enterprise Edge the usual way using Unified Manager and from the navigation tree, click **System.** The system name is displayed in the System Name box.

3. Click **Find Now**.

4. Double-click on the computer icon.
The NortelDT folder is displayed.

5. Open the NortelDT folder.

6. Open the Unified Manager IE Client or Unified Manager Netscape Client folder, depending on which Internet browser you use to access Enterprise Edge Unified Manager.

7. Double-click on the **Setup.ex** icon to install the client software on your computer.

Accessing Unified Manager through the Preinstalled Client Home Page

Tips
To access Unified Manager through the Preinstalled Client Home Page, you must first preload the Java class files on your PC. See Preloading Java class files on your workstation.

1. Lauch you browser and enter your Enterprise Edge IP address followed by port 5800. For example: http://10.10.10.1:6800
The Enterprise Edge Unified Manager initial page is displayed.

2. From Enterprise Edge home page, click the P**reinstalled Client Home Page** hyperlink.

3. Click the **Configure** button to access Unified Manager.

Logging off Enterprise Edge

To log off Enterprise Edge:

1. Choose **Enterprise Edge** in the navigation tree.
   The **Logoff** menu is enabled.

2. From the **Logoff** menu, click **Logoff**.

   A message appears that asks you to confirm your request to log off.

3. Click **Yes** to log off.

Rebooting the Enterprise Edge server

To reboot the Enterprise Edge server:

1. Choose **System** in the navigation tree.
   The Logoff menu is enabled.

2. On the **Logoff** menu, click **Reboot**.

   A message appears that asks you to confirm your request to reboot.

3. Click the **Yes** button to reboot.

Shutting down Enterprise Edge System

To shut down the Enterprise Edge System:

1. From the navigation tree, choose **System**.
   The Logoff menu is enabled.

2. On the **Logoff** menu, click **Shutdown**.
   A message appears that asks you to confirm your request to shut down the system.

All Enterprise Edge services stop when performing system shutdown
Performing a system shutdown stops all Enterprise Edge applications and services, including IP telephony. Active IP telephony calls fall back on the PSTN if you have programmed your system to do so.

3. Click the **Yes** button to shut down the system.
   A Shutdown process status window is displayed and the **Done** button is enabled.

4. Click the **Done** button.
   When the shutdown is completed, your browser loses the connection with Enterprise Edge.

Tips
The Enterprise Edge system automatically restarts 45 seconds after the Power LED turns off. Disconnect Enterprise Edge power cord from the AC outlet if you do not want the system to restart withing this period of time.

Licensing

The Licensing heading in Unified Manager allows you to view Enterprise Edge unique System Identification Number.

To view the System Identifier:

1. Choose **System**, **Licensing**.
   The System Identifier is displayed in the System section.

Entering the software keycodes

To enable software packages other than the base package, you need a security keycode. Each security keycode contains three eight-digit numbers. For information about how to obtain System Identification numbers, see the *Enterprise Edge Software Keycode Installation Guide.*

To enable a software package:

1. Select **System**, **Licensing**.

2. On the Configuration menu, click **Add a keycode**. A dialog box appears.

3. In the **Keycode** box, type the 24-digit number in the following format: xxxxxxxx-xxxxxxxx-xxxxxxxx.

4. Click **Save.**

Configuring system settings

You configure your system settings using the **Group** menu selection in the upper-left corner of your screen.

1. Choose **Group** and then choose **System** or **Comprehensive**.

2. Click the **System** key to expand the navigation tree.
   The Licensing and Identification headings appear.

3. Click **Identification**.
   The Identification window is displayed.

4. Use the following table to configure the System Identification settings:

Setting	Definition
System Name	Allows you to assign a name to the Enterprise Edge system. Each Enterprise Edge system on a network must have a unique name. The name must not exceed 15 characters in length and must not contain special characters like "/;,".
Description	Shows a description of the Enterprise Edge system.
Date	Allows you to set the current date. Because the value for the date changes, save the changes by pressing TAB as soon as the new date is entered.
Time	Allows you to set the current time. Because the value for the time keeps changing, save the changes as soon as the new time is entered. Use the 24-hour format to set the time. The seconds field is optional.
Time Zone	Allows you to select the local time zone for your system.
Country	Allows you to select the country you are in.
Current Domain Name	Allows you to enter the name of the domain on which your Enterprise Edge system is currently registered. You must add Enterprise Edge to the domain controller before you add the current domain name.
New Domain Name	Allows you to enter the new name of the domain on which your Enterprise Edge system is registered. You must add Enterprise Edge to the domain controller before you enter the new domain name.
Next Hop to NT Domain Controller for TAPI	Enter the IP address of the next hop to reach the domain controller for TAPI.

Note: For information on configuring Enterprise Edge resources and services, refer to Configuring Enterprise Edge Resources on page 45, and Configuring Enterprise Edge Services on page 83.

System registration

When your Enterprise Edge system is installed and operational, it registers specific information with a Tivoli Management Region (TMR) server. The goal of registration is to build a customer profile containing system inventory information which can then be used to bring you enhanced support and value-added services.

Note: To allow automatic registration, you must connect the system to the internet. In North America, you also have the option to connect your system to an analog line (PSTN) to establish a dial-up connection using the v.90 modem. The system makes repeated call attempts every 24 hours until it connects to the Tivoli server. The repeated attempts the system makes to make a connection are transparent to your use of the system. For information on how to connect the installed v.90 modem to a telephone line, refer to the *Enterprise Edge Installation and Maintenance Guide*.

Basic registration using Internet Access

For basic system registration using the public Internet, the system needs direct access to the Internet (without going through a firewall). If access to the Internet is through a firewall, the following configuration rules must be set on the firewall:

- For traffic coming from the Enterprise Edge, allow all UDP and TCP traffic to the Nortel Tivoli Gateway (192.122.98.36) on ports above 1023.
- From the Nortel Tivoli Gateway (192.122.98.36) allow TCP traffic to Enterprise Edge on port 9495.

Basic Registration using v.90 modem (North America only)

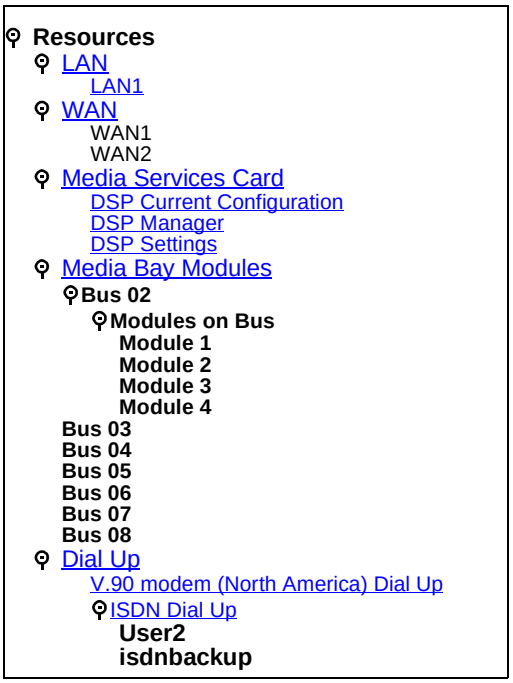
Refer to the *Enterprise Edge Installation and Maintenance Guide* for information on how to setup the Enterprise Edge v.90 modem.

The following information is automatically collected:

- System ID
- System Hardware list
- System Software list
- Operating system details

Configuring Enterprise Edge Resources 4

This chapter provides information on configuring Enterprise Edge resources. The following shows the programming map for Enterprise Edge telephony and networking resources:



Note: The resources listed on this table may not correspond exactly at the resources available on your Enterprise Edge system.

For information on how to view the Enterprise Edge resources available on your system, refer to Viewing Enterprise Edge resources on page 45.

Viewing Enterprise Edge resources

Unified Manager lets you view and configure Enterprise Edge networking resources including LAN, WAN, and dial up resources such as ISDN or V.90 modem (North America). To view the networking resources your Enterprise Edge system supports:

1. On the **Group** menu, click **Resources** or **Comprehensive**.

2. On the navigation tree, click **Enterprise Edge,** and then click **Resources**. The available Enterprise Edge resources appear in a table format.

The Resources table contains the following information:

Attribute	Description
Name	Provides a list of available resources.
Status	Shows the operating status of each resource.
Version	Shows the software version of each resource.
Description	Provides a description of the interface card for each resource.

LAN

Enterprise Edge is equipped with an Ethernet/802.3 network interface card which supports the IEEE 802.3 Ethernet frame format. The Ethernet connection uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage the access to the physical media.

The Enterprise Edge Ethernet interface card supports the following features:

- 100 BASE – TX with RJ-45 connector
- 10 / 100 Auto Sense
- Full Duplex
- Fast LAN-to-LAN routing (when using more than one LAN cards)
- LAN traffic smoothing

Viewing LAN resources and configuring global LAN attributes

Enterprise Edge Unified Manager shows all available LAN resources. If your Enterprise Edge server is equiped with two LAN interface cards, Unified Manager displays all available LAN resources and numbers each one (LAN1, LAN2).

To view the available LAN resources and configure global LAN attributes:

1. Select **LAN** from the navigation tree. Unified Manager displays the global LAN Parameters and the Resources table showing available LAN cards.

Configuring LAN resources

Setting LAN global parameters

1. Click on the **Resources** heading to expand the navigation tree.
   The available resouces appear.

2. Click **LAN**.
   The Lan Parameters and Resources windows appear.

3. Set your global LAN parameters according to the following table:

Attribute	Description
Fast Routing (Between LANs)	Allows you to enable or disable fast routing to improve LAN-to-LAN routing performance. This feature is for an Enterprise Edge system equipped with two LAN cards. At the same link speed, a smaller packet size means more packets to forward. Use a lower traffic threshold. For more information on Fast Routing, see Guidelines to configure LAN to LAN traffic smoothing. Permitted values: **Enabled** or **Disabled** Default: **Disabled**
Decrement TTL	When Fast Routing is enabled, Decrement TTL lets you decrement the time-to-live (TTL) value in the IP header of packets as they travel from LAN to LAN. Decrement TTL lets you increase processing time for each fast-routed IP packet, which reduces CPU cycles. This feature is used when other routers or special applications on the network connect to the LAN interfaces. Permitted Values: **Enabled** or **Disabled** Default: **Disabled**
Traffic Smoothing (In Mbps)	Lets you set the rate, in Mbps, at which the LAN driver receives packets from the LAN interface. The main purpose of this feature is to limit the number of host CPU cycles spent on LAN-to-WAN packet forwarding. Normally, LAN drivers operate at link speed, which implies that the driver forwards packets as fast as possible until there is no packet in the receiving buffer. Permitted values: **5**, **10**, **15**, **20**, **25**, **30**, **35**, **40**, **45**, **50, Disabled** Default: **40**

Guidelines to configure LAN to LAN traffic smoothing.

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1500 bytes
Fast Routing enabled	40 mbps	50 mbps	50 mbps	50 mbps	Not needed	Not needed
Fast Routing disabled or LAN-to-WAN routing	10 mbps	15 mbps	30 mbps	50 mbps	50 mbps	50 mbps

Note: The settings shown in the table above ensure data routing uses a maximum of 60 to 70 percent CPU cycles (Celeron 366MHz processor).

Note: If the LAN to WAN link speed is 10 mbps, selecting higher traffic smoothing parameters has no impact on packet forwarding, which the system still performs at a link speed of 10 mbps.

Configuring a LAN interface

LAN1

To configure LAN1 or any other LAN interface:

1. Click the **LAN** navigation key to expand the navigation tree.
   The available LAN interfaces appear.

2. Click **LAN1**. Unified Manager displays the LAN Summary screen for LAN1.

3. Configure the LAN1 attributes according to the following table.

Attribute	Description
IP Address	Enter the IP address of the LAN interface in the following format: 255.255.255.255. If you do not know your LAN interface IP address, contact your system administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask of the LAN interface in the following format: 255.255.255.255. If you don't know your subnet mask address, contact your system administrator or your Internet service provider.
Physical Address	Shows the physical address of the LAN interface.
Description	Provides a description of the network interface card supporting the LAN connection.
Version	Shows the version of the LAN interface card.
Speed	Shows the speed of the connection to the LAN interface.
Connection Type	Lets you select a type of connection to the LAN interface. The following values are supported and are interpreted as follows: **Auto Sense**: The LAN interface uses the auto negotiation protocol to choose the maximum possible speed of the connection. Depending on the connected device, the LAN can choose 100 MB or 10MB, full-duplex or half-duplex. **10 MB Half**: The speed is set to 10 Mbit/s and mode to half-duplex. **10 MB Full**: The speed is set to 10 Mbit/s and mode to full-duplex. **10 MB Auto**: The speed is set to 10 Mbit/s and the mode (half-duplex or full-duplex) is automatically selected by the interface, using the auto negotiation protocol. The **10MB Auto** connection type limits the maximum traffic coming into Enterprise Edge to 10 Mbit/s, and enables the auto negotiation feature for easier interconnection. Limit the incoming traffic if you notice that the bursty traffic from the connected LAN is degrading the quality of voice calls carried through VoIP over the WAN. Though the LAN traffic gets lower priority in Enterprise Edge, a high incoming traffic to the Enterprise Edge server can result in service interruptions in the system, which degrades the quality of voice calls carried as VoIP. **100 MB Half**: The speed is set to 100 Mbit/s and mode to half-duplex. **100 MB Full**: The speed is set to 100 Mbit/s and mode to full-duplex. Default value: **Auto Sense**
Status	Shows the current status of the LAN connection. The possible states are: **Up**: The resource is operational. **Down**: The resource is not operational.

Note: Consult your System Administrator for the appropriate configuration information before changing the settings.

Note: Because the Enterprise Edge WAN interface has a maximum bandwidth of 1.544 Mbit/s (T1) or 2.048 Mbit/s (E1), setting the LAN connection speed to 10 Mbit/s does not reduce performance. However, the CPU is more efficient if you limit your incoming traffic to 10 Mbit/s. To increase your CPU performance, set the connected external LAN hub or switch to **10 Mbit/s** or to **Auto Sense**.

Note: If you enable LAN Traffic Smoothing, the connection type defaults to Auto Sense and there is no requirement on the external LAN hub or switch.

To view LAN performance:

1. From the LAN1 summary screen, on the menu, click **Performance** and then click **LAN Graph**.
   The LAN Graph: Statistic Chart screen is displayed.

2. On the menu, click **Performance** and then click **LAN Table**.
   The LAN Table: Statistic Table screen is displayed.

WAN

WAN Overview

A WAN (wide area network) is a geographically dispersed data communication network. The term WAN distinguishes a broader data communication structure from a local area network (LAN). A WAN can be privately owned or rented, but usually connotes the inclusion of public (shared user) networks.

Enterprise Edge is equipped with a SDL WAN Series 500 interface card with two serial synchronous ports (Europe), or a SDL WAN Series 550 interface card with one T1 port (with integrated CSU/DSU) and one serial synchronous port (North America). Each port from the WAN interface provides a primary WAN connection (WAN1, WAN2). The serial synchronous port supports the following:

- North America: V.35
- Europe: V.35 (Upper Sync Port) and X.21 (Lower Sync Port)
- Maximum line speed: 8 Mbit/sec.

Enterprise Edge provides primary and backup WAN links through dial-up connections using a V.90 modem (North America) or ISDN BRI/PRI. For information on V.90 modem or ISDN connections, see Dial Up. Net Link Manager provides continuous WAN connection status monitoring. For information on Net Link Manager, see Net Link Manager on page 229.

Permanent WAN Connection

The permanent WAN connection is exposed as a dedicated network adapter. The permanent link supports frame relay or Point-to-Point protocol (PPP) at the link layer. The link protocol used depends on the existing network or on the service you buy from your Internet service provider. The two ports provided by the SDL WAN interface card can be independently configured to run frame relay or PPP.

Frame Relay

Enterprise Edge supports frame relay in *group* mode. That is, for each physical port (serial sync or T1 port), there is one IP address for all PVCs (permanent virtual circuits). The available Data Link Control interface numbers are 0-1023. Of the 1023 PVCs, 16 are reserved. The maximum number of PVC's allowed is 1008.

For a frame relay network, Enterprise Edge supports the Frame Relay Forum standard FRF.9 compression protocol with the standard STAC compression algorithm. Enterprise Edge software performs the compression. For information on enabling or disabling WAN data compression, see WAN Data Compression on page 50.

Point-to-Point-Protocol (PPP)

Point-to-Point Protocol (PPP) is a full-duplex transmission protocol for communication between two computers using a serial interface, typically a personal computer connected by telephone line to a server. For example, your Internet service provider (ISP) can provide you with a PPP connection so that the ISP's server can respond to your requests, pass them on to the Internet, and return your requested Internet responses to you. PPP uses the Internet protocol (IP).

Enterprise Edge supports PPP Compression Control Protocol (CCP) (RFC 1962) with STAC compression algorithm. This compression is done by Enterprise Edge software and can be enabled or disabled using a parameter in PPP configurations. For information on WAN data compression, see WAN Data Compression on page 50.

WAN Data Compression

Enterprise Edge provides a WAN Data Compression feature. You can use data compression on permanent WAN connection and on backup WAN connection. By default, WAN Data Compression is enabled on Enterprise Edge. WAN Data Compression can be enabled or disabled from the Setting WAN Frame Relay Parameters screen or from the WAN PPP Parameters screen, depending on your system configuration.

On a permanent WAN connection, Enterprise Edge supports the following data compression protocol:

- Frame Relay Forum standard FRF.9 data compression protocol with de facto standard STAC compression algorithm
- PPP Compression Control Protocol (RFC 1962) with STAC compression algorithm

On dial-up WAN connections, Enterprise Edge supports the following data compression protocol:

- Microsoft Point-to-Point Compression (MPPC), RFC 2118

Viewing WAN Resources

Enterprise Edge lets you view available WAN resources.

To view available WAN resources:

1. From Unified Manager, under Resources, click **WAN**. The Resources section displays the WAN interfaces (WAN1, WAN2) in a table format.

Setting global WAN parameters

If PPP is the link protocol for a WAN interface (WAN1 or WAN2), you can use an authentication process to identify the user requesting a network connection. The authentication process involves creating a list of user names and assigning passwords using the PPP Password List. Enterprise Edge uses the information on the list to verify and confirm the identity of the user. Only those users whose names appear on the PPP Password List can access the network. The PPP Password List configuration lets you add, modify or delete an item on the list.

To create a PPP Password List:

1. From the WAN Resources section, scroll down to the PPP Password List.

2. From the menu click **Configuration** and select **Add PPP User&Password**. The PPP Password List dialog box appears.

3. In the **P#** box, type the number of the list item. For example, if you are adding the first item on the list, the **P#** is **P1**.

   Note: If you type an item number which already exists in the list, the following message appears "You tried to add a row with existing key". Assign a new number to the item to want to add to the list.

4. In the **PPP User Name** box, type the user name associated with the computer you want Enterprise Edge to identify as a valid network user.

   Note: You must overwrite the default user name **User** with the user name you want to add to the list.

5. In the **PPP Password** box, type the password you want to assign to the user defined in the **PPP User Name** box. The password can contain a combination of lowercase and uppercase letters and numbers.

6. Click **Save** to save your settings.

To modify an existing item on the PPP Password List:

1. From the list, click the item you want to modify. The selected item is highlighted.

2. From the menu, click **Configuration** and select **Modify PPP User&Password**. The PPP Password List dialog box appears.

3. Make the necessary changes.

4. Click **Save** to save your changes.

To delete an item from the PPP Password List:

1. From the list, select the item you want to delete. The selected item is highlighted.

2. From the menu, click **Configuration** and select **Delete PPP User&Password**. A dialog box appears to ask "Are you sure you want to delete this row?" Click **Yes.**

Configuring WAN Summary Parameters

1. Click the WAN navigation key to expand the navigation tree.

2. On the navigation tree, click **WAN1** or **WAN2.** Unified Manager displays the following screens: WAN Line Parameters (if you are configuring a T1 port [North America only]), WAN Frame Relay or PPP Parameters (depending on the link protocol selected), and PVC Congestion Control screens.

   Note: Clicking the WAN1 or WAN2 navigation key causes the key to disappear. You must click WAN1 or WAN2 to access the WAN Summary screen.

3. Use the attributes in the following table to configure Enterprise Edge WAN Summary settings:

Attribute	Description
IP Address	Enter the IP address of the WAN interface. The WAN IP address must be in the following format: 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
SubNet Mask	Enter the subnet mask address of the WAN. The subnet mask IP address must be in the following format: 255.255.255.255. You can obtain this information from your system administrator or your Internet service provider.
Physical Address	Shows the physical address of the WAN interface.

Attribute	Description
Description	Provides a description of the network interface card that supports the WAN connection.
Port	Shows the port type of the WAN interface.
Version	Shows the version of the WAN interface.
Speed	Shows the operational speed of the WAN interface.
Status	Shows the current resource status of the WAN interface. The possible states are: **Up**: The resource is operational. **Down**: The resource is not operational.
Link Protocol	Lets you select a WAN link protocol. The options are **Frame Relay** or **PPP** protocol. The default is **Frame Relay**. If you change the link protocol, the configuration screen changes to include fields corresponding to the link protocol you choose. To ensure proper operation, always refresh the page by clicking **View** and then **Refresh**. The link protocol to choose depends on the existing network or on the service you buy from you Internet services provider.
Compression	Lets you enable or disable data compression. The possible values are: **Enabled**, **Disabled** The default is **Disabled**.
Frame Size	Lets you specify the maximum frame size for the layer-2 packet carried on this port. The default is **1600**.

4. Press the **TAB** key to save your settings.

Note: Unified Manager refreshes the link protocol screen according to the choosen protocol. Your choice of protocol depends on the existing network or on the service you buy from your Internet service provider. Frame relay is the default link protocol. If you change the link protocol the following message appears "Reminder! Previous setting requires rebooting the system to take effect. Please reboot the system..." Click **OK**.

Reboot the system
You must remember to reboot your system for the changes you made to the link protocol to take effect. You can continue Enterprise Edge Resources configuration and reboot the system at a convenient time.

Setting WAN Line Parameters

The WAN Line Parameters screen is displayed when configuring a T1 port (North America only). Enterprise Edge supports T1 and fractional T1. Refer to the **Port** box on the WAN Summary Parameters screen to see which type of port your are configuring.

1. Use the information provided in the following table to set the WAN Line Parameters:

Attribute	Description
Channel Rate	Lets you set the data transmission rate for each of the DS0 channels in the T1 line. Possible values are **64K** or **56K**. The default value is **64K**.
Clock Source	Lets you set an internal or external T1 clock source. Possible values are **External** or **Internal**. The default value is **External**.
Frame Type	Lets you set the type of framing the T1 line supports. Possible values are **ESF** or **SF(D4)**. The default value is **ESF**. Use the setting your T1 service provider recommends.
Line Coding	Lets you set the type of encoding used in the T1 line. Possible values are **B8ZS** or **AMI**. Use the setting your T1 service provider recommends.
Line Polarity	Lets you set **Normal** or **Inverted** line polarity in the T1 line. Select **Inverted** only if Line Coding is set to **AMI**.
Pulse Density	Lets you control whether the DSU/CSU maintains the minimum level of 1s on the line for AMI encoding. Possible values are **Enabled** or **Disabled**. Default value is **Disabled**.
Channel List	Lets you create a list of T1 channels used when using fractional T1. You can list each channel numbers or provide a range of numbers separated by a comma or hyphen. The channel list can contain a mix of ranges and individual channel numbers. For example, a valid channel list format is 3,5,6,10-15,18,20-23. To use all the available T1 channels, type **All.** Your T1 service provider can give you this information. Default value is **All**.

Note: Always use the same frame type as your service provider.

Note: Always use the same line coding method as your service provider.

2. Press the **Tab** key to save the settings.

Setting WAN Frame Relay Parameters

If you chose frame relay as your link protocol, set the WAN Frame Relay Parameters.

1. Use the information in the following table to set the WAN Frame Relay Parameters:

Attribute	Description
LMI Type	Lets you set the type of local management protocol used on this link. The link management type must be the same as the one used by the frame relay service provider. The available options are **Original LMI, ANSI T1.617 Annex D** or **ITU-T Q.933 Annex A**. The default setting is **Original LMI**.
Polling Interval	Lets you set an interval, in seconds, between LMI status inquiry messages. The polling interval must be the same as the one used by the frame relay service provider's switch. Possible values are between **5** and **30** seconds. The default setting is **10**.
Full Enquiry Interval	Lets you set the maximum number of LMI Status Enquiry messages sent before sending a Full Status Enquiry request. This value must match the corresponding value set in the frame relay service provider's switch. Possible values are between **1** and **255** (in seconds). The default setting is **6**.
Error Threshold	Lets you set the maximum number of consecutive failures permitted in LMI Status Enquiry before dropping the link. It is also the number of successful consecutive LMI Status Enquiry messages that must be received before marking a link as operational. Possible values are between **0** and **MAXINT**. The default value is **3**.
Monitored Events	Lets you set the number of events sampled for making decisions about the error threshold. This value must be set to a higher number than the value set in the **Error Threshold** box. Possible values are a number between **0** and **MAXINT**. The default value is **4**.
DS Code	Lets you set the Differentiated Services code (DSCode) recognized by the frame relay driver for traffic prioritization. This value is a mask value. When an IP packet is sent, the frame relay driver checks if the packet's DSCode field (in the IP header) has any of the bits defined in the **DS Code.**
Compression Enabled PVCs	Lets you create a lists of PVCs on which data compression is enabled. Type the list of PVCs for which data compression is enabled. The value can be a comma-separated list of DLCI numbers.You can define a range of DLCIs by inserting a hyphen between the lower and the upper boundaries. A list can contain individual DLCI numbers and DLCI ranges. If data compression is enabled, compression and decompression operations are performed on the data going to and coming from the PVCs enumerated on this list.
Access Rate	Lets you set, in kbps, the maximum access rate on the interface running frame relay. The frame relay congestion control engine uses this value to limit or shape traffic. The **Access Rate** value is determined using the T1 channels available for data communication on the port attached to this interface and their data rates.

2. Press the **Tab** key to save the settings.

PVC Congestion Control

If frame relay is your link protocol, you must configure PVC Congestion Control. If PPP is your link protocol, there are no PVC Congestion Control settings to configure.

1. Use the following table to set WAN PVC Congestion Control:

Column	Description
Entry (CC#)	Lets you define each congestion control entry on the interface. A congestion control entry must use the following format: CC2, where the prefix 'CC' is followed by a number. Each entry must use a different number. For example, 'CC2' is a valid congestion control entry. Enterprise Edge requires that you use consecutive numbers when entering congestion control entries. If you do not use consecutive numbers, the system adjusts them to be consecutive. If you add an existing entry, the existing entry is modified with new values. When you modify an entry, the name cannot be changed.
DLCI	Lets you enter the data link connection identifier (DLCI) number of the PVC on which to perform congestion control. A DLCI must be configured for congestion control to be performed. Enterprise Edge uses one-second intervals to measure this parameter.
CIR	Lets you set, in kbits, the committed information rate. The CIR is the carrier guarantees that the router transmits over a predetermined time interval when congestion is not present. Contact your service provider for correct setting. Enterprise Edge uses one-second intervals to measure this parameter.
Committed Burst (bC)	Lets you define the number of bits, in kbits, the router transmits over a specified time interval if congestion is present. As a rule this value is set for 1/4 the value of the CIR. Enterprise Edge uses one-second intervals to measure this parameter.
Excess Burst (Be)	Combined with the committed burst rate, lets you set, in kbits, the maximum number of bits the router transmits over a predetermined time interval if there is no congestion. The combined value of committed burst and excess burst must be less than or equal to the line speed.

To add PVC congestion control:

1. On the menu, click **Configuration,** and then click **Add PVC Congestion Control**.

2. In the **Entry (CC#)** box, type the entry “CCxx” where “xx” is a unique integer.

3. In the **DLCI** box, type the DLCI number.

4. In the **CIR (kbps)** box, type the CIR in kbps.

5. In the **Committed Burst BC (kbits)** box, type the committed burst in kbits.

6. In the **Excess Burst BE (kbits)** box, type the excess burst in kbits.

7. Click the **Save** button to save the entries.

To modify a PVC congestion control entry:

1. Select the entry you want to modify in the PVC Congestion Control table

2. On the menu, click **Configuration,** and then click **Modify PVC Congestion Control**.
   The PVC Congestion Control dialog box appears.

   Note: If you have not selected a PVC Congestion Control entry, an error message appears saying "Please select a row in the Table".

3. Click any box that requires modification and make the changes.

4. Click the **Save** button to save the modifications.

To delete a PVC congestion control entry:

1. Click the entry you want to delete in the PVC Congestion Control table.

2. On the menu, click **Configuration,** and then click **Delete PVC Congestion Control**.
   A message prompts you to confirm the deletion.

   Note: If you have not selected a PVC Congestion Control entry, an error message appears saying "Please select a row in the Table".

3. Click the **Yes** button to delete the PVC congestion control entry.

WAN PPP Parameters

If you chose PPP as your link protocol, set the WAN PPP Parameters screen.

1. Use the following table to set the WAN PPP parameters:

Attribute	Description
LCP Keep Alive Interval	Lets you define at which interval, in seconds, to send a keep alive signal when there is no regular traffic on the PPP link. The default value is **10**.
LQR Interval	Lets you define at which interval, in 1/100 second, to perform link quality monitoring.
Allowed Authentication	Lets you specify if a remote user can use PAP or CHAP or if the remote user is restricted to use CHAP only.

Attribute	Description
Cisco's Encapsulation Mode	Lets you enable or disable the Cisco compatibility mode.

2. Press the **Tab** key to save your settings.

WAN performance

To access the WAN Primary Link performance graphs and tables for a particular WAN interface:

1. In the navigation tree, select **WAN1** or **WAN2**.

2. On the menu, click **Performance**, **WAN Graph**.
   The WAN Graph: Statistic Chart appears.

3. On the menu, click **Performance, WAN Table**.
   The WAN Table: Statistic Table appears.

Dial Up

Enterprise Edge lets you create and use dial up connections for Remote Access Service (RAS) or dial-on-demand network access. RAS lets you access Enterprise Edge remotely by making an IP connection using an ISDN BRI/PRI line or the Enterprise Edge V.90 modem (North America). Once connected to the Enterprise Edge system, you can access all IP-based system management operations.

Enterprise Edge also supports dial-on-demand for primary and backup WAN connections. Primary and backup WAN connections can use an ISDN BRI/PRI line or a V.90 modem (North America).

Configuring RAS Server TCP/IP

1. Click the **Resources** key to expand the navigation tree.

2. Click **Dial Up**.
   The RAS Server TCP/IP Configuration screen appears.

3. Use the following table to configure the RAS Server TCP/IP settings:

Attribute	Description
Allow Network Access	Lets you give dial up access to the entire network (**Yes**) or to restrict access to Enterprise Edge only (**No**). When using dial up for dial-on-demand WAN connection (as a primary or back up WAN connection), set **Allow Network Access** to **Yes**. When using dial up for remote system management purposes only, set to **No**.

Attribute	Description
Static IP Address Pool	Lets you set the IP address Enterprise Edge assigns when a remote site dials into the Enterprise Edge system. The default value is **10.10.10.5**
Address Mask	Lets you set the IP address mask corresponding to the IP address range. The IP addresses from the static address pool then reserved for assignment to remote sites. The default value is **255.255.255.240**

4. Press the **TAB** key to save your settings.

ISDN Dial Up

Enterprise Edge supports ISDN Dial Up for dial-on-demand WAN access. You have the choice to use ISDN BRI/PRI as your primary WAN connection or as a back up for your permanent WAN connection.

Tips
To use an ISDN dial-up connection, you must first configure your system for ISDN. For more information, refer to Appendix B: ISDN Overview. If your system is already configured to support ISDN, make sure you configure a Data Module for ISDN dial up connection. For more information, see Configuring a data module.

Tips
After you have created an ISDN dial up interface, you must use Net Link Manager to select which type of network connection the system must use for primary and backup connection.

Creating an ISDN dial up interface

1. Click the **Resources** key, and then click the **Dial Up** key to expand the navigation tree.
   The existing ISDN interfaces are listed and the **Add** button at the top of the navigation tree is enabled.

2. Click the **Add** button located over the navigation tree.
   The Add ISDN dialog box appears.

3. In the **(Dial In) Name** box, type the name of the interface you are creating.

Add backup to Name
If you are creating an ISDN interface to use as a backup for a permanent WAN connection, the **(Dial In) Name** must contain the string "backup". For example, "ISDNbackup" is a valid name if you want to use an ISDN connection as a WAN backup connection.

4. In the **Password** box, type a password.

5. In the **Confirm Password** box, type your password again.

6. In the **Channel** list, select the channel the connection must use.

7. Click **Save** to save your settings.
   The newly created ISDN interface is displayed under **ISDN**.

Configuring an ISDN interface

To configure an ISDN interface:

1. Under **Resources, Dial Up, ISDN,** click on the interface you want to configure.
   The ISDN Summary, ISDN Link Parameters, ISDN Access Parameters and ISDN Channel Characteristics screens are displayed.

2. Use the following table to configure the ISDN Summary settings:

ISDN Summary:

Attribute	Description
Interface	Shows the name of the ISDN interface selected.
IPAddress	Lets you set the IP address of the ISDN interface when it connects. You can set a fixed IP address for the dial-up interface. You can select **RemoteAssigned** to indicate that Enterprise Edge must obtain an IP address from the remote end. The address obtained depends on the RAS server to which Enterprise Edge connects. The default value is **RemoteAssigned**.
Description	Shows a description of the interface.
Status	Lets you view and set the ISDN interface resource status. Possible values are: **Up**: the ISDN interface is currently connected. Also used to force the interface to initiate a connection. **Down**: the ISDN interface is not currently connected. **Enabled**: the ISDN interface is enabled for use. **Disabled**: the ISDN interface is currently disabled.

You cannot select an ISDN interface that is set to “RemoteAssigned” as the Local Gateway IP for the VoIP Gateway.

ISDN Link Parameters

Use the following table to set the ISDN Link Parameters:

Attribute	Description
Dial Retries	Lets you set the number of times the systems attempts to connect before considering the connection nonoperational. The default value is **3**.
Dial Interval	Lets you set the interval, in seconds, between connection attempts. The default value is **60**.
IP Header Compression	Lets you enable or disable IP header compression. The feature must be enable at both ends of the connection. The default value is **Enabled**.
Software Compression	Lets you enable or disable software compression. When enabled, all dial-up connections use Microsoft Point-to-Point Compression (MPPC). The default value is **Disabled**.
PPP LCP Extensions	Lets you enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.
Disconnect Time	Lets you set, in seconds, the interval during which the ISDN interface disconnects when there is no traffic.

3. Scroll down to the ISDN Access Parameters screen.

ISDN Access Parameters

1. Use the following table to set the ISDN access parameters:

Attribute	Description
Authentication	Lets you select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: when selected the Challenge Handshake Authentication Protocol (CHAP) is used first and if the receiving end of the link declines, PAP is used to authenticate the link. **EncryptedOnly**: when selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Lets you enable or disable link authentication in both directions.
Dial-Out User ID	Lets you define a user name and password that the link must use to authenticate itself when dialing out to another router.

2. Scroll down to the ISDN Channel Characteristics screen.

ISDN Channel Characteristics

The ISDN Channel Characteristics shows the default characteristics for the channel you selected when you created the ISDN interface. The following ISDN Channel Characteristics table provides a description of each ISDN channel characteristics:

Attribute	Description
Row(R#)	Identifies the number of the item in the ISDN channel list.
Port	Shows the channel selected for this ISDN interface. The channel shown here is the channel you selected when you created the ISDN interface.
Phone 1	Lets you enter the phone number to use to make an ISDN connection to the network or to Enterprise Edge. If needed, include area codes and all necessary digits to dial an external number. The phone number must contain only numerical digits only (no alphabetical or other characters are allowed).
Phone 2	Lets you enter an alternate phone number to use to make the ISDN connection. If needed, include area codes and all necessary digits to dial an external number. The phone number must contain numerical digits only (no alphabetical or other characters are allowed).
Line Type	Lets you specify if the line is a 64K or 56K digital line.
Fallback	Lets you specify whether or not to fall back to a slower speed if unable to connect at the previously set speed.

To add an ISDN channel to the ISDN Channel Characteristics list:

1. From the **Configuration** menu, choose **Add ISDN Channel.**
   The ISDN Channel Characteristics property sheet appears.

2. Use the table under ISDN Channel Characteristics to configure the channel characteristics settings.

To modify the characteristics of an existing ISDN channel:

1. From the ISDN Channel Characteristics screen, click on a row.
   The row is highlighted.

2. From the **Configuration** menu, select **Modify ISDN Channel.**
   The ISDN Channel Characteristics property sheet appears.

3. Make the necessary changes. See the table under ISDN Channel Characteristics for a description of each characteristic.

4. Click the **Save** button to save your settings.

To delete an ISDN channel from the ISDN Channel Characteristics list:

1. In the ISDN Channel Characteristics screen, click on a row.
   The row is highlighted.

2. From the **Configuration** menu, select **Delete ISDN Channel.**
   The Select an Option screen appears, asking you if you want to delete the selected row from the list.

3. Click the **Yes** button.

Deleting an ISDN interface

To delete an ISDN interface:

1. Click the **ISDN** key under **Resources**

2. Click the name of the interface you want to delete. The interface name is highlighted.

3. Click the **Delete** button located at the top of the navigation tree. A dialog box asks you "Are you sure you want to delete this node?".

4. Click **Yes**.

V.90 modem (North America) Dial Up

Enterprise Edge is equipped with an internal V.90 modem which connects to your phone line with a RJ-11 connector. The V.90 modem has the following features:

- V.90 56 kbps ITU standard
- V.34 33.6 kbps ITU standard
- V.42/MNP 2-4 error control
- V.42 bis/MNP 5 data compression
- Compatible with ITU and Bell Standards from 56 kbps down to 1200 bps

Note: The modem is capable of receiving at a maximum speed of 56 kbps and transmitting at a maximum speed of 31.2 kbps. Because of FCC regulations, receiving speed is limited to 53 kbps. Current line noise can impact the speed of the modem.

The V.90 modem WAN connection always uses PPP as the link layer protocol. For correct operation, the link must be connected to a remote access server (RAS).

Enterprise Edge supports the following authentication features:

- Password Authentication Protocol (PAP)
- Challenge Authentication Protocol (CHAP)

Configuring V.90 modem interface for dial up WAN backup connection

Tips

Remember to set Dial Up global parameters before creating modem dial up interfaces. For information on setting Dial Up global parameters, see Configuring RAS Server TCP/IP.

The same modem is shared between the remote dial-in for system administration and the backup WAN link. The WAN backup function is not available if a break in the WAN permanent connection occurs while a system administrator is connected to Enterprise Edge.

The V.90 modem is used for WAN backup connection. To configure V.90 modem interface:

1. Click **Resources** to expand the navigation tree.

2. Click the **Dial Up** key to expand navigation tree.

3. On the navigation tree, click the **V.90** key to see available modem interfaces. Enterprise Edge comes with a default modem backup interface called **ModemBackup**. The TivDialup interface, which is also listed under **V.90,** is reserved for Tivoli system management.

4. On the navigation tree, click ModemBackup. A screen displays the following: Modem Summary, Modem Link Parameters, Modem Access Characteristics

Modem Summary Parameters

1. Use the following table to set the Modem Summary Parameters:

Attribute	Description
Interface	Shows the name of the modem interface selected.
IP Address	Lets you set the IP address of the modem interface when it connects. Users can set a fixed IP address for the dial-up interface. If a fixed address is specified, Enterprise Edge uses the address to the receiving end. Users can select **RemoteAssigned** to indicate that Enterprise Edge must obtain an IP address from the remote end and use it. The address obtained depends on the RAS server to which Enterprise Edge connects. The default value is **RemoteAssigned**.
Description	Shows a description of the interface.
Version	Shows the version of the modem subsystem.

Attribute	Description
Status	Lets you view the modem interface resource status and to enable or disable the modem interface. The possible states are: **Up**: the auto WAN backup service is enabled and the dial-up link is currently active. **Down**: the auto WAN backup service is enabled and the dial-up link is currently disconnected. **Enabled**: the interface is enabled for use by the auto-backup server. **Disabled**: the auto WAN backup service is disabled.

2. Press the **Tab** key to save the settings.

Modem Link Parameters

1. Use the following table to set the Modem Link Parameters:

Attribute	Description
Telephone Number	Lets you type a telephone number to use to connect using the modem interface. If needed, include area codes and all necessary digits to dial an external number.
Alternate Telephone Number	Lets you type an alternate number to use to connect using the modem interface. Include area codes and all necessary digits to dial an external number.
Connect Rate	Lets you specify the initial speed (in bits per second) for the modem to connect. Set to the maximum permissible value for best results. Permitted values: 57600, 38400, 19200, 9600, 4800. Note: This is the initial rate; the actual rate is always negotiated.
Dial Retries	Lets you set the number of attempts the system must make when trying to connect before considering the connection nonoperational The default value is **3**.
Dial Interval	Lets you set the interval, in seconds, between successive connection attempts. The default value is **60**.
Speaker Mode	Lets you enable or disable the speaker during initial link establishment.
IP Header Compression	Lets you enable or disable IP header compression. To function, the receiving end must also use this feature.
Software Compression	Lets you enable or disable data compression in the software, instead of the modem. For dial-up connections, Unified Manager uses Microsoft Point-to-Point Compression algorithm (MPPC).
Hardware Compression	Lets you enable or disable data compression in the hardware instead of the software.
PPP LCP Extensions	Lets you enable or disable the following PPP Link Control extensions: Time-Remaining and Identification. The default value is **Enabled**.

2. Press the **TAB** key to save the settings.

V.90 Modem Access Parameters

1. Use the following table to set the V.90 Modem Access Parameters:

Attribute	Description
Authentication	Lets you select the authentication type for the link. The options are **AllowClearText** or **EncryptedOnly**. **AllowClearText**: when selected the Challenge Handshake Authentication Protocol (CHAP) is used first and if the receiving end of the link declines, PAP is used to authenticate the link. **EncryptedOnly**: when selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication process.
Two Way Authentication	Lets you enable or disable link authentication in both directions.
User ID (name password)	Lets you define a user name and a password that the link uses to authenticate itself when dialing out to another router.

2. Press the **TAB** key to save the settings.

Guidelines for Using Remote Dial-in

Consider the following guidelines when using remote dial-in:

- The same modem is shared between the remote dial-in for administration and the backup WAN link. If a remote administration user is connected while the primary link breaks, the automatic backup function does not occur.
- While using the back-up interface, Enterprise Edge always calls. Enterprise Edge does not answer an incoming call from a router.

Media Services Card

Enterprise Edge applications consume Digital Signal Processor (DSP) resources. DSP resources are controlled by software (the number of ports or services that are available to any application) and hardware (the number of MSPECs) installed. Each system is preconfigured with a default DSP resource allocation based on the number of MSPECs installed. However, you may need to change the DSP resource allocation using the DSP Manager if you:

- replace an MSPEC
- purchase more software

For more information on configuring DSP resource allocation, refer to:

- Rules for configuring DSP resource allocation on page 67
- DSP Current Configuration on page 68
- DSP Manager on page 68
- DSP Settings on page 69

Rules for configuring DSP resource allocation

The following rules apply when configuring DSP resource allocations:

- When no MSPECs are installed, 8 Voice channels can be configured
- The system can be configured with a maximum of:
  - 16 Voice channels
  - 2 FAX channels
  - 8 WAN ports
  - 8 VoIP trunks
- Each MSPEC can be configured with a maximum of:
  - 2 VoIP trunks
  - 12 Voice channels
  - 1 FAX channel
  - 8 WAN ports
- Eight WAN ports will be configured automatically if there are available MSPEC resources
- If both Voice channels and VoIP trunks are configured on the same MSPEC, a maximum of 2 Voice channels can be configured
- If both Voice channels and WAN ports are configured on the same MSPEC, a maximum of 4 Voice channels can be configured
- The following ports and channels cannot be configured together on the same MSPEC:
  - WAN and VoIP
  - WAN and FAX

The following table lists some allowable combinations of channel types and identifies the default configuration for some types of feature codes on a 4 MSPEC system.

	Voice	VoIP	FAX	WAN	Default configuration when feature code is
1	8	8	0	0	8 VoIP trunks or 8 VoIP trunks and FAX
2	16	6	1	0	6 VoIP trunks and FAX
3	10	6	0	8	6 VoIP trunks
4	16	4	2	0	4 VoIP trunks and FAX
5	16	4	1	8	
6	16	4	0	8	4 VoIP trunks
7	16	2	2	8	2 VoIP trunks and FAX
8	16	2	0	8	2 VoIP trunks
9	16	0	2	8	
10	16	0	0	8	no feature codes entered

DSP Current Configuration

To view the current DSP resource allocation:

1. Choose **Resources**, **Media Services Card**, **DSP Current Configuration**.

   The DSP Current Configuration window displays the number of channel types running on each MSPEC. For example, the default configuration might include 4 Voice channels and 8 WAN ports running on MSPEC number 4 (DSP-4 on the table). For more information on allowable MSPEC configurations, refer to the table above.

DSP Manager

The DSP Manager is used to change the DSP resource allocation currently running on the system. To change the DSP resource allocation, use the following procedure:

1. Choose **Resources**, **Media Services Card**, **DSP Manager.**

   The DSP Manager window is displayed, showing the configuration that you can edit. In addition, the DSP Configurations window displays a table showing the Current, Default and Custom configurations.

   Current configuration is the configuration that is currently running on your system. Default configuration contains the default values preprogrammed for the number of MSPECs showing. Custom configuration is the configuration that you are programming into your system. You must reboot the system for the Custom configuration to become to Current configuration.

2. Select **Custom** from the **Edit** menu.

3. Enter the appropriate values in the boxes according to the Rules for configuring DSP resource allocation on page 67.

   Note: At any time during this step, you can revert back to the default or current configuration by selecting **Default** or **Current** from the **Edit** menu.

4. Select **Validate** from the **Configuration** menu.

   The system will notify you if your configuration is valid by displaying a message in the Last Status box.

5. Select **Submit** from the **Configuration** menu.

   The **Last Status** box displays a message indicating that the custom configuration has been submitted and that a system restart is required. The next time you restart your system, the custom configuration will be loaded.

DSP Settings

The system DTMF length may need to be adjusted because of certain detection errors. For example, some cellular phone tones are closer to the short DTMF millisecond range. If a company is having trouble with the cellular phone connections, it may be necessary to change the DTMF length to 30 milliseconds.

To change the DTMF length:

1. Choose **Resources**, **Media Services Card**, **DSP Settings.**

   The DSP Settings window displays the DTMF length.

2. Click in the box and change the DTMF length to a value between 30 and 60.

3. Press the Tab key to save your settings.

Media Bay Modules

The Media Bay Modules heading lets you view and change settings for trunk modules installed in Enterprise Edge. The following illustration shows a detailed view of the Media Bay Modules programming map and the attributes that appear for each different module type.

Note: Depending on which Media Bay Module your system is equipped with, the settings and parameters available may vary.

- **Media Bay Modules**
  - Bus **02 - 07**
    - **Modules on Bus**
      - Module **1**
        - Module type **PRI**
        - Low line/loop
        - High line/loop
        - Protocol
        - Protocol type
        - NSF extension
        - B channel selection sequence
        - Clock source
        - Overlap receiving
      - Call-by-call service selection
        - **Foreign Exchange**
        - **Inwats (800)**
        - **Switched Digital (SDS)**
        - **Inter...**
        - **Nine Hundred (900)**
      - T1 Parameters (North America only)
        - CO fail
        - Interface levels
        - Framing
        - Internal CSU
        - CSU line build
        - Line coding
      - Provision lines
        - **Line xxx**
          - Status

- **Media Bay Modules (cont'd)**
  - Bus **02 - 07**
    - **Modules on Bus**
    - **Ports on Bus**
      - Module **1**
        - Module type **Loop**
        - Low line/loop
        - High line/loop
        - Disconnect timer
      - Module **1**
        - Module type **T1**
        - Low line/loop
        - High line/loop
        - Disconnect timer
        - Answer timer
        - Clock source
      - T1 Parameters (North America only)
        - CO fail
        - Interface levels
        - Framing
        - Internal CSU
        - CSU line build
        - Line coding
      - Module **1**
        - Module type **BRI-ST**
        - Low line/loop
        - High line/loop
        - Protocol
        - Clock Source
        - Overlap receiving
      - Module **1**
        - Module type **DPNSS**
        - Low line/loop
        - High line/loop
        - Clock source
        - Local num len
        - Maximum transits
      - Module **1**
        - Module type **DASS2**
        - Low line/loop
        - High line/loop
        - Clock source

To enable or disable any of the buses on the Enterprise Edge system:

1. Under the **Resources** heading, click the **Media Bay Modules** key.
   Buses 02 to 08 are displayed.

2. Select the bus you wish to disable.
   Information about the bus is displayed and the **Configuration** menu option is enabled.

3. On the **Configuration** menu, select **Disable**.
   The system prompts you to confirm your request.

4. Click the **OK** button to disable the bus.

Bus

Bus 01 is reserved for the MSC card. Because there is no hardware programming required for the MSC card, bus 01 is not displayed. You can view and perform maintenance operations on Bus 01. For more information, see Maintenance on page 259.

For a detailed description of the various Media Bay Modules and proper hardware configurations, see the *Enterprise Edge Installation and Maintenance Guide*.

Note: Because the voice over IP (VoIP) functionality resides on the MSC card, it is not necessary to program any hardware settings for it. The **Trunk mode** is automatically set to VoIP for lines 001 to 014. For more information, refer to Lines on page 108.

To configure a bus type:

1. Choose **Resources**, **Media Bay Modules**.

2. Click a **Bus** (Bus 02 to 07).

   Note: Bus 08 is reserved for configuring a data module, which provides a soft router connection to a remote router. The functionality for this feature is on the Media Services Card, not in a discrete media bay module. For information about programming a data module, see Configuring a data module on page 79.

3. From the **Programmed Bus Type** list, choose a bus type.

4. Press **Enter**.

   The choice of Programmed Bus Type available depends on the hardware unit that is installed. The following table shows the type of bus available for each hardware unit.

Bus Type	Hardware unit
Station module	Digital Station Media Bay Module (EE-DSM 16 or EE-DSM32)
Analog station module	Analog Station Media Bay Module (EE-ASM 8)
Trunk module	Digital Trunk Media Bay Module (EE-DTM) CLID Trunk Media Bay Module (EE-CTM) BRI S/T Media Bay Module (EE-BRIM S/T)
Fiber Expansion Module	Set module, Analog Station Module, UK analog LEC, BRI-U2, BRI-U4, BRI-ST

Module

The Module heading lets you configure settings for the module. Options displayed depend on the type of Media Bay Module installed in your system and the Module type you select.

To program a module:

1. Choose **Resources**, **Media Bay Modules**, **Bus 02-07**, **Ports on Bus** and **Module 1** to access the module configuration settings.

2. Click a Module type: **Loop**, **PRI**, **BRI-ST, DASS2, DPNSS** or **T1,** and press **Enter**.

   Note: To provision PRI lines, see Provision lines on page 81.

3. Configure the card settings according to the following table:

Attribute	Description
Low/line loop	Automatically assigned based on the card type and the module number. For more information, see page 73. Values: View only
High line loop	Automatically assigned based on the card type and the module number. For more information, see page 73. Values: View only
Disconnect timer[1]	Lets you specify the duration of an Open Switch Interval (OSI). For more information, see page 74. Values: 60, 100, 260, 460, or 600 milliseconds (Default: 460)
Answer timer[2]	Lets you set the minimum duration of an answer signal before a call is considered to be answered. Values: 1, 2, 3, 4, or 5 seconds (Default: 2)

Attribute	Description
Protocol[3]	Lets you define a trunk protocol. For more information, see page 74. Values: NI-2, DMS100, DMS250, AT&T4ESS, SL-1, Euro, Q-Sig
Protocol type[3]	Lets you define a protocol type. This settings applies to the SL-1 private networking protocol only. For more information, see page 74. Values: User (Slave), Network (Master) Default: User (Slave)
NSF Extension[3]	Lets you define the Network Specific Facilities (NSF) information element. If the prompt **Clear Routes** is displayed, click **Yes** to confirm your selection. For more information, see page 74. Values: None, WATS, ALL
B-channel selection sequence[3]	Lets you define how B-channels are selected. For more information, see page 75. Values: Ascending Sequential, Descending Sequential
Clock Source[4]	Lets you designate which EE-DTM acts as a primary or secondary timing slave or a Timing Master. The Clock Source may also be programmed on BRI T-loops or NT loops. For more information, see page 75. Values: Primary, Secondary, Timing Master

Notes:
1 Applies to Loop and T1 card types only.
2 Applies to T1 card types only.
3 Applies to PRI card types only, NI2 protocol only.
4 Applies to PRI and T1 card types only.

Note: There must be an EE-DTM installed if you want to program PRI or T1 trunk lines. The EE-DTM is automatically disabled and re-enabled when you change the card type. There is no need to manually enable and disable it.

Low line/loop High line/loop

Low line/loop and High line/loop settings are automatically assigned according to the settings in the following table. Note that Buses 6 and 7 are reserved for the Companion mobility option if Companion is included in the system.

Card Type	Bus 02	Bus 03	Bus 04	Bus 05	Bus 06	Bus 07
T1 (Card 1)	211-234	181-204	151-174	121-144	91-114	61-84
PRI (Card 1)	211-233	181-203	151-173	121-143	91-113	61-83
Loop (Card 1)	211-214	181-184	151-154	121-124	91-94	61-64
Loop (Card 2)	219-222	189-192	159-162	129-132	99-102	69-72
Loop (Card 3)	227-230	197-200	167-170	137-140	107-110	77-80
Loop (Card 4)	235-238	205-208	175-178	145-148	115-118	85-88

Note: PRI on a T1 carrier has 23 lines (for example, Bus 2 has L211-233). PRI on an E1 carrier has 30 lines (for example, Bus 2 has L211-l240).

Disconnect timer

Disconnect timer (North America only) lets you specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO).

You must enable disconnect supervision by changing the **Trunk mode** attribute. Under the Telephony Services sub-heading, choose Lines and Line/trunk Data. See Trunk/line data on page 111 for more information.

Protocol

Enterprise Edge supports a number of different trunk protocols used by different service providers and markets. Supported protocols are listed in the table below.

ISDN Service	Protocol
PRI-T1	NI-2, DMS100, DMS250, AT&T4ESS, SL-1
PRI-E1	QSIG, Euro, Sl-1
BRI (North America)	NI
BRI (Europe)	Euro, QSIG

Protocol type

When you select SL-1 protocol, an additional setting, Protocol type, appears. Because SL-1 protocol is a private networking protocol, you have the option of designating an Enterprise Edge node as a Network (Master). The default setting is User (Slave). In public network configurations, the CO is generally considered the Network side or Master.

Protocol	Type
NI-2, DMS100, DMS250, AT&T4ESS	Public protocols
SL-1 (premium feature)	Private protocol

NSF Extension

If you select the NI-2 protocol and you are using Call-by-Call services, you must specify how Enterprise Edge should handle the NSF (Network Specific Facilities)

The table below summarizes the NSF Extension settings recommended for each switch type.

Central Office	NSF Extension Setting
DMS100	None
Siemens ESWD, Lucent 5ESS	WATS
GTD5, DMS10	ALL
The Network Specific Facilities (NSF) information element is used to request a particular service from the network. When you select **NONE**, the NSF extension bit is not set for any service. When you select **WATS**, the NSF extension bit is set for unbanded OUTWATS calls. When you select **ALL**, the NSF extension is always set for all CbC services.	

B-channel selection sequence

B-channel selection sequence lets you select either **Ascending Sequential** or **Descending Sequential** depending on your service provider. You should choose the opposite setting of your service provider.

If all lines for two EE-DTMs (configured as PRI) are in the same PRI pool, then both cards must be set to use the descending B-channel selection sequence. As a result, the service provider must use ascending sequential sequence.

The B-channel selection sequence for BRI QSIG is always set to Descending on Enterprise Edge, so it must set to Ascending on the service provider.

Clock Source

Clock Source lets you designate which of the systems' Digital Trunk Modules (EE-DTMs) obtains the timing reference from the network to be used for synchronization.

Systems with digital interfaces need to synchronize to the network in order to function. Synchronization is done in a hierarchical way, where each device (switch) obtains the network clock from the device above it in the synchronization hierarchy and passes the network clock to the device below it in the synchronization hierarchy. The synchronization levels are referred to as strata. BRI modules can also be used for the timing reference.

Enterprise Edge systems are stratum 4E equipment and are usually used as termination points in a network.

For each EE-DTM, choose one of the following settings: **Primary**, **Secondary**, or **Timing Master**.

Primary reference

The EE-DTM obtains the timing reference from the network and the system synchronizes to it. This is the default value for the first EE-DTM in Enterprise Edge. If the system is configured with an EE-DTM (configured as PRI), the setting should be set to Primary.

Secondary reference

The EE-DTM acts as a standby reference. If there are excessive errors on the primary T1 reference link, or the EE-DTM designated as primary reference fails, the second EE-DTM will obtain the timing reference from the network to be used for system synchronization. This is the default value for the second EE-DTM in Enterprise Edge.

Timing Master

The EE-DTM does not obtain timing from the network, but transmits the systems timing to equipment connected to it.

Changing clock source may disconnect calls.

Changing the clock source for your system may cause your system to restart itself, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

Tips

In most T1 network configurations, you need one EE-DTM configured as PRI to act as a primary reference. The only application where you might not have a PRI EE-DTM designated as a primary reference is in a network where your Enterprise Edge system is connected back-to-back with another switch using a T1 link or PRI link. If the other switch is loop-timed to your Enterprise Edge system, your EE-DTM configured as PRI can be designated as a timing master.

If your Enterprise Edge system has two EE-DTMs, you cannot assign both EE-DTMs as primary reference or both EE-DTMs as secondary reference.

You can only have one primary reference and one secondary reference per system. You can have a T1 or PRI(T1) or PRI(E1) or BRI as clock source.

Call-by-call service selection

By default, incoming calls are routed based on the Called Party Number. The last 'N' digits of the called party number are used as Received Digits to find a target line (where 'N' is the Received Number Length).

For example, the incoming calling party number is 800-555-1234. The received digit number length is 4, and the result is 1234. These last four digits are used to route the call.

Depending on the protocol and the service, alternate routing maps may be defined.

1. To change the incoming call routing for a service, select a different service under **Protocol:, Call by Call Routing, FX:**

   The first applicable service for the given protocol is displayed. In this example, the service is **FX**.

2. Change the mapping that is applied to incoming calls of this service type to obtain the received digits. In all cases, the received digits are used to find a target line or to activate Remote Access.

   None: No mapping is applied. The last 'N' digits of the Called Party Number are used as received digits. Note that if there is no called party number (may occur with some FX calls) the call will ring at the incoming trunk's Prime set.

   All: Lets you define the received digits used for all calls with this service type, regardless of the called party number or service identifier (SID). For this option, all calls with this service type on this PRI will ring the same target line.

   Map table: Lets you associate different received digits with different calls of this service type depending on the call party number and/or the service identifier. Incoming calls that do not match any entry defined in the map table will ring at the prime set. Depending on the service type and the protocol, you may be able to map the called party number (By number) and the service identifier (SID). The following table shows the different options.

	Service				
Protocol	**FX**	**800**	**I-800**	**SDS**	**900**
NI-2	SID	By number	N/A	N/A	N/A
DMS-100	SID	SID or By number	N/A	N/A	N/A
DMS-250	SID	SID or By number	N/A	N/A	SID or By number
4ESS	N/A	By number	By number	By number	By number

Note: This setting is available for T1 trunks configured as T1 E&M. See Trunk/ line data on page 111 for more information about configuring trunk types.

T1 Parameters (North America only)

The T1 Parameters heading appears for card types that have been configured as T1 or PRI. It lets you define a number of settings that are dependent on your T1 service provider settings.

To program T1 Parameters:

1. Choose **Resources**, **Media Bay Modules**, **Bus 02-07**, **Modules on Bus, Module 1**, and **T1 Parameters**.

2. Configure the T1 parameters according to the following table:

Attribute	Description
CO fail	Lets you select the carrier failure standard used by your T1 or PRI service provider. Consult your T1 or PRI service provider for the proper setting. Values: TIA-547A or TR62411 (Default: TIA-547A)
Interface levels	Lets you define a loss plan setting. For more information, see page 78. Values: ISDN or PSTN (Default: ISDN)
Framing	Lets you select the framing format used by your T1 or PRI service provider: Extended Superframe (ESF) or Superframe (SF). Contact your T1 or PRI service provider for the proper setting. (SF or Superframe is sometimes known as D4.) Values: ESF or SF (Default: ESF)
Internal CSU	Lets you turn the internal T1 channel service unit on or off. For more information, see page 79. Values: On or Off (Default: On)
CSU line build	Lets you set the gain level of the transmitted signal. This setting only appears when the Internal CSU is set to On. Values: 0, 7.5, or 15 dB (Default: 0)
DSX1 build	Lets you set the distance between Enterprise Edge and an external channel service unit. This setting only appears when the Internal CSU is set to Off. Contact your service provider for the proper settings. Values: 000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet (Default: 000-100)
Line coding	Lets you define the encoding signals on a T1 line. Select the standard used by your T1 service provider. Contact your T1 service provider for the proper setting. Values: B8ZS or AMI (Default: B8ZS)

Interface levels

Interface levels defaults to the ISDN loss plan setting.

Find out if your Enterprise Edge system is connected to a central office (CO) with digital network loss treatment (ISDN I/F levels) or analog network loss treatment (PSTN I/F levels) by checking with your telecommunications service provider.

The ISDN setting requires digital access lines (DAL) that have digital network loss treatment. On a DAL network, it is the PBX, rather than the CO, that administers the dB loss. DALs may have ISDN signaling or digital (such as T1 and so on) signaling. The loss plan follows the Draft TIA-464-C loss plan, which uses a send loudness rating (SLR) of 8 dB. To have DAL network loss treatment on a line with digital signaling, you must contact your service provider.

The PSTN setting requires analog access lines (AAL) that have analog network loss treatment and digital signaling. On an AAL(D) network, the CO administers the dB loss.

The loss plan follows the Draft TIA-464-C loss plan. The ISDN loss plan uses a send loudness rating (SLR) of 8 dB and a receive loudness rating (RLR) of 2 dB. The PSTN loss plan uses an SLR of 11 dB and an RLR of -3 dB. Choosing the wrong setting may affect voice quality, either too loud or too soft.

Internal CSU

Internal CSU lets you turn the internal T1 channel service unit on or off. The channel service unit gathers performance statistics for your T1 lines or PRI with public interface. Contact your service provider for the proper settings.

Note: You must disable the EE-DTM before you can change this setting. See Media Bay Module status on page 279 for details.

You can view the performance statistics for your T1 lines in Maintenance under the CSU stats heading. If you set the internal CSU off, there must be an external CSU connected to your T1 lines.

E1 Parameters (Europe)

Enterprise Edge does not provide E1 parameters. If your Enterprise Edge is connecting to a network using E1 trunks, make sure CRC4 checking is enabled at the other end.

Configuring a data module

Module 08 is reserved for a data module. The data module provides connectivity for a soft router through Enterprise Edge from facilities such as T1 and BRI. The remote soft router server only needs to be powered up and running for the feature to be available. Enterprise Edge automatically configures the Module type as a Data Module, sets the Data module type to Baystack, and sets the IP address. Baystack is currently the only soft router supported on Enterprise Edge.

Viewing the data module settings

Use the following procedure to view the current settings for the data module.

1. Under **Resources, Media Bay Modules,** choose **Bus 08**.

Note: Before you can configure the data module for fixed access, you must first configure an EE-DTM module as T1(see Module on page 72) and you must set the trunk type to Fixed data channel (see Trunk/line data on page 111).

Programming the BayStack settings

When you select the BayStack data module, the following configuration settings appear:

- IP address
- Switched access
- Line assignment

- Line pool access
- Fixed access

IP address

This is the IP Address of the BayStack data module.

Switched access (PRI & BRI)

You can assign ISDN lines to the BayStack data module to provide:

- normal data network access for the data module
- dial-up backup and overflow bandwidth (additional channels or trunks) as needed

The line assignment and line pool access settings are displayed in **Switched access**.

Line assignment

Use the following procedure to assign one or more lines to the BayStack data module for incoming data transmission:

1. In **Line Assignment**, enter the number of the trunk or a target line you need to assign to the BayStack data module.

   The status of the line appears as assigned to the current data module, unassigned, or assigned to another data module. You can assign a trunk directly to the BayStack data module.

2. Select **Unassigned** or **Assigned**.

   If the line is assigned to another data module, you can reassign it to the current data module.

3. Enter the Dial-In Number for the line (up to 24 digits). The number must match the Dial-In Number entered for the line and channel in BayStack data module programming.

4. Assign additional lines to the BayStack data module as required.

Line pool access

Use the following procedure to give the BayStack data module access to a line pool for outgoing data transmission:

1. The settings for access to the line pools are displayed in **Line pool access**.

2. Select the line pools in the list to provide access to the BayStack data module.

   You must program line pool access when you select the switched access settings for the BayStack data module. To use PRI line pools, program the BayStack data module to use a destination code.

For more information about programming switched access, see the data module *Installer Guide*.

Provision lines

The Provision lines heading lets you provision and deprovision ISDN lines. It also lets you disable PRI channels.

Provision a T1 line

1. Choose **Resources, Media Bay Modules**.

   The window displays Buses 02 through 08.

2. Choose the bus (Bus 02 to 07) associated with the module you want to provision.

   Note: Bus 08 is reserved for a data module and has no lines to provision.

3. Expand the **Modules on Bus** heading.

   The modules on this bus are displayed.

4. Choose the module (for example, Module 1) you want to provision.

5. Expand **Provision lines**.

   All the available lines are displayed.

6. Click the line you want to provision.

7. From the Status box, click **Provisioned**.

Provision a PRI or BRI line

PRI lines are provisioned by default. BRI loops/lines are provisioned by default only in the international markets.

Deprovision a line

Deprovisioning all of the lines on an EE-DTM does not disable the module.

Note: BRI loops/lines are deprovisioned by default in the North American market.

1. Choose **Resources, Media Bay Modules**.

   The window displays Buses 02 through 08.

2. Choose the bus (Bus 02 to 07) associated with the module you want to provision.

   Note: Bus 08 is reserved for a data module and has no lines to provision.

3. Expand the **Modules on Bus** heading.

   The modules on this bus are displayed.

4. Choose the module (for example, Module 1) you want to provision.

5. Expand **Provision lines**.

   All the available lines are displayed.

6. Choose the line you want to deprovision.

7. From the Status box, click **Deprovisioned**.

Disable a PRI Channel

PRI channels can be disabled; however, there is no association between a line number and a B-channel. Disabling of a B-channel can be done when you have fractional PRI. For more information, refer to Link Status on page 301.

Configuring Enterprise Edge Services 5

This chapter describes the programming procedures for the many Enterprise Edge Services, from Telephony to Firewall Filters. Note that a number of other programming steps are also required to get the system up and running.

Programming order

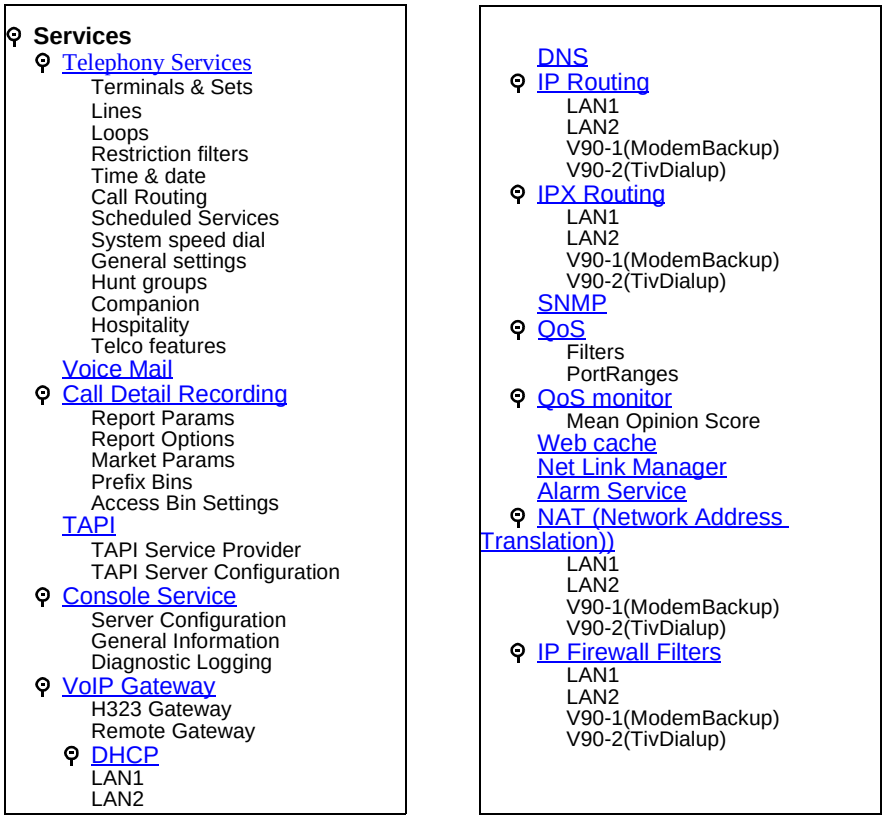
Program Enterprise Edge system components in the following order to ensure optimum operation:

1. Media Bay Modules (hardware); see Media Bay Modules on page 69.
2. Lines; see Lines on page 108
3. Terminals & sets; see Terminals & sets on page 90
4. General Settings; see General on page 91
5. Companion (N.A. only), Hunt Groups, Hospitality; see Companion on page 177, Hunt groups on page 170, Hospitality on page 183
6. System Speed Dial and Telco Features; see System speed dial on page 145, Telco features on page 187
7. Passwords; see COS Passwords on page 160

Programming affects system operation.
Only a qualified system administrator should perform startup, installation and maintenance programming. Many of the settings affect correct system operation.

Programming Services

This is the Services programming map:



You can configure Services attributes under the following headings in the **Services** section of Unified Manager:

- Telephony Services on page 87
- Voice Mail on page 188
- Call Detail Recording on page 188
- TAPI on page 188
- Console Service on page 189
- VoIP Gateway on page 189
- DHCP on page 192
- DNS on page 199
- IP Routing on page 200
- IPX Routing on page 208
- SNMP on page 216
- QoS on page 220
- QoS monitor on page 227

- Web cache on page 228
- Net Link Manager on page 229
- Alarm Service on page 232
- NAT (Network Address Translation) on page 232
- IP Firewall Filters on page 235

Viewing Enterprise Edge Services

To access Services attributes from Unified Manager:

1. On the menu, click **Group,** then **Services** (or click **Comprehensive** to display all options).

2. To expand the navigation tree, click the **Enterprise Edge** key (⊙) and **Services**. The Enterprise Edge **Services** table appears, with the name, status, version, and description of the available services. This table also appears when you select **Enterprise Edge, System**.

3. Click the **Services** key to expand the tree. The first listing is **Telephony Services**.

Viewing all Services

To view the status, version and description of all Services:

1. Click on the **System** heading.
   The Item, Resources and Services screens appear.

To Enable or Disable a Service

2. On the **Configuration** menu click **Modify Services**.
   The **Services** dialog box appears.

3. Click **Enabled** or **Disabled** in the Status box.

4. Click Save.

Statuses

Status	Description
Enabled	Indicates that the resource or service is currently operating. When the component is enabled, the component can assume any of its operational statuses.
Disabled	The component is disabled from operation. None of the component's operational statuses are valid in this state.
Paused	The component is enabled and is running but is currently not accepting additional service requests.
Up	This value is read-only. It indicates that the component is enabled and is operating normally. For a component like a network interface, this means the interface is enabled and connected to a valid link. For a service like DHCP, it means that the service is enabled and is currently running normally When the current status is Up, setting it to Enabled or Continue (where available), is a no-operation. Setting it to Disabled disables the service, by shutting it down and then disabling it. Where available, setting it to Paused pauses the service
Down	This value is read-only. This value indicates that the user has enabled the component, and the component is unable to operate in an Up state because of normal or abnormal, internal or external errors. For example, if a network interface is in a Down state because of no connection to an actual physical link, it is a normal, external error. If a service like DHCP service is in a Down state because of internal errors, it is an abnormal, internal error. When the current status is Down setting it to Enabled attempts to bring it to 'Up' state again. In an error still exists it may stay at a Down state. Setting it to Disabled disables the service. Where available, setting it to a Paused or continued state fail as the service is not yet running.
Enabled	This value is write-only. This value never appears when read. For a service that is enabled, one of its operational statuses (that is, Up or Down) appears when its Status field is read. When this value is set, it indicates that the user wants to enable the corresponding component and bring it to an Up state. It is probable that the first happens. The second action depends on the component. For a network interface, the Up state does not happen unless user connects a link to the interface. For a service this may not happen only if the system encounters an error of some kind during the requested action.
Disabled	This value can be either read or set. When read, this indicates that the component is disabled from operation. When set, it indicates the same, in addition to taking the component to a Down state before disabling.
Paused	This value can be either read or set. When read, this indicates that the service is enabled and is given the command to pause. When set, it indicates the same, pausing the service further.
Continue	This value can only be set. It can be set only when the service in a Paused state. It resumes paused service.

Telephony Services

This section describes the procedures to configure Enterprise Edge **Telephony Services**, found under the **Services** heading in Unified Manager.

Telephony Services allows you to program and manage all the voice components associated with Enterprise Edge. You can set up lines and trunks, define settings for individual telephones, and customize your telephone network to suit your requirements. From Unified Manager, expand **Services** and **Telephony Services** to view the subheadings.

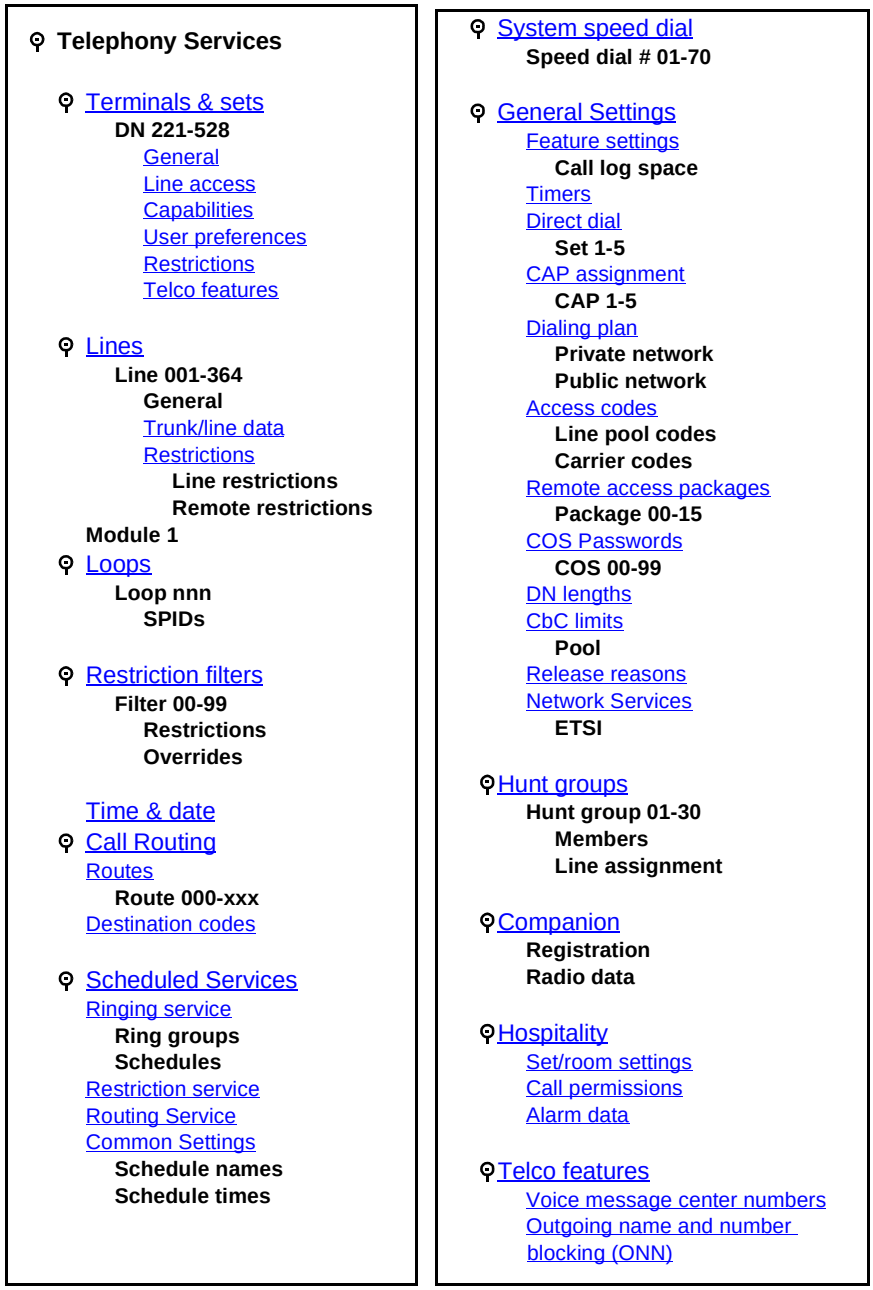
The table below summarizes the Telephony Services subheadings. Note that provisioning and diagnostics information is in Maintenance on page 259.

Note: To jump to any section for more information, click the blue, underlined text. The information is automatically displayed.

Terminals & sets	Allows you to assign settings to each telephone.
Lines	Allows you to assign settings to each trunk and target line.
Loops	Allows you to configure settings for BRI loops.
Restriction filters	Allows you to apply restriction filters for external calls.
Time & date	Allows you to set the display format for both date and time.
Call Routing	Allows you to define how calls are routed on your Enterprise Edge system.
Scheduled Services	Allows you to create services, such as night ringing, routing and restrictions, for making external calls.
System speed dial	Allows you to create speed dial codes that can be used by any telephone in the system.
General Settings	Allows you to change system-wide settings.
Hunt groups	Allows you to create and manage hunt groups.
Companion	Allows you to assign settings for portable telephones.
Hospitality	Allows you to assign Hospitality settings.
Telco features	Allows you to assign settings for external voice message services.

When you select **Telephony Services**, the **Tools** menu becomes active. The **Tools** menu allows you access to the Backup and Restore tool. For more information on using the Backup and Restore tool, refer to Backup and restore on page 260.

The following illustration shows an overview of the Telephony Services programming that is accessible through Unified Manager.



Enhanced 911 (E911) Configuration

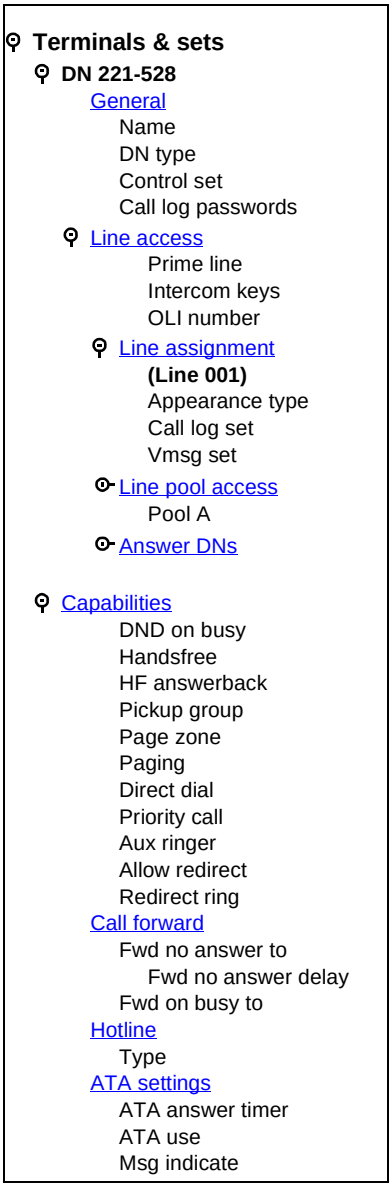
Government rules vary for support of Enhanced 911 (E911) dialing service by Customer Premises Equipment. Legislation may require that the Customer Premises Equipment give a more precise location of the source of a 911 call than the billing address of the central office line. Consult your service provider about the laws and regulations.

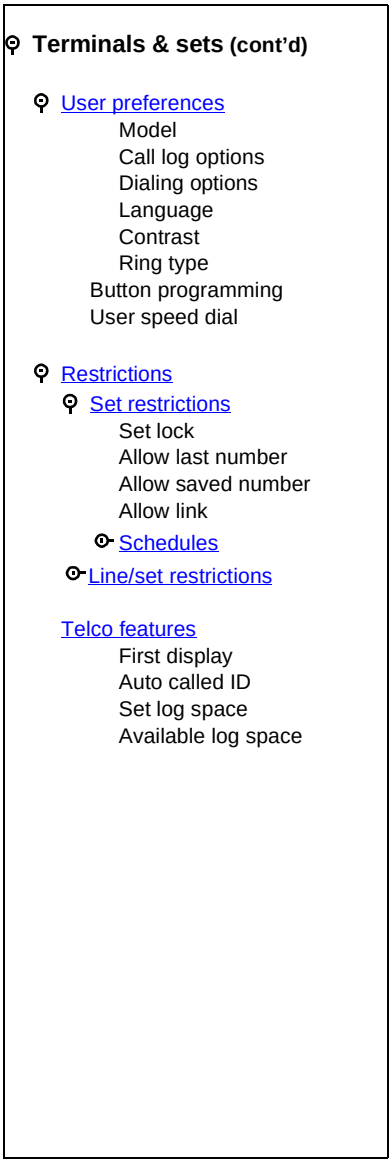
Use the following configuration rules when installing the Enterprise Edge system, to assure compliance with local regulations:

- When equipped with PRI trunks, Enterprise Edge can deliver the Calling Line ID of a telephone dialing 911 through the Public Switched Telephone Network, if the proper programming has been implemented and PRI trunk service has been installed by the service provider. If you are using ISDN PRI, implement OLI programming and Business Name programming to add the Set ID to the CLASS information.
- By default, Restriction Filter 02 is assigned to all sets on startup. There are no restrictions applied in Restriction Filters 02-99. Restriction Filter 01 has restrictions, but 911 is an Exception for this filter. For information on how to change the Restrictions, refer to Restrictions on page 103.
- When using other trunk interfaces, you can assign separate line pools to groups of telephones in different areas (for example, in different buildings, floors or sections).
- Be careful when using the Set Relocation feature. You may have to reprogram the line pool access to send the right location on 911 calls.
- Configure the 911 destination code to dial out over a Normal Schedule in all applicable Service Modes, as this is the default route should any other programmed routing attempts fail. When using PRI interfaces, make sure all sets can use the PRI line pool that the Normal Schedule route uses.

Terminals & sets

The Terminals & sets heading allows you to assign settings to each telephone. The following shows a detailed view of the Terminals & sets navigation tree.





Copying settings from one telephone set to another

The Copy command allows you to duplicate programming for a telephone and apply it to another telephone, a range of telephones or all the telephones on the system.

To copy telephone settings:

1. Choose **Services, Telephony Services, Terminals & sets**.
2. Click the telephone set (DN 221-528) with the settings you want to copy. If necessary, choose a subheading to refine your selection.
3. On the **Edit** menu, click **Copy**.
4. Choose the data type you want to copy, **System data** or **System+user data**.
5. Click **Single, Range** or **All** from the Copy type list.
6. Type the DN number of the set or the range of sets (nnn-nnn) where you want to copy the settings. You do not have to fill in this box if you chose **All** in the Copy type list.
7. Click the **OK** button.

General

The General attributes allows you to assign the name, the DN type, a control set, and the Call log password for a set.

Name

The default name for a telephone is its DN. You can change it to a more descriptive name.

To assign a name to a telephone:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Click **General**.
4. In the **Name** box, type a name up to seven characters, and then press **Enter**.

   Note: The name can be a combination of letters and numbers.

DN type

The DN type attribute allows you to choose the set type: ISDN set or portable set. For Enterprise Edge desk sets, you can view but you cannot change the DN type.

To change the DN type:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Click the **General** heading.
4. Click a **DN type**: ISDN or Portable.

   Note: In North America, DNs 469 to 500 are Portable sets and DNs 501 to 528 are ISDN sets by default.

Control set

The Control set attribute allows you to define a DN that will act as a control set. By default, DN 221 is the control set for all telephone sets (DNs). A control set can turn Scheduled Services, such as Restriction Service on and off for the telephones assigned to it. For more information about services, see Scheduled Services on page 138.

You can assign several control sets for your system but you can only assign one control set per DN.

Tips

You must program external lines and telephones with a control set to use the three kinds of Scheduled Services: Ringing, Restriction, and Routing Services.

The recommendation is to have one control set for all lines and a different control set for all telephones (DNs).

You can turn on a service manually or automatically for all telephones controlled by a given control set, but you cannot combine schedules. In other words, a service can only be active as normal service or one of the six schedules at any one time. You can have several schedules active, as long as they are using different services.

To assign a control set to a DN:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Click **General**.
4. In the **Control set** box, type the DN number and press **Enter**, or click **None**.

Call log passwords

Call log passwords setting allows you to clear an individual's Call log password. This is useful if someone forgets the password and you need to reset it. Select the set DN and leave the box blank or enter a new password. The user can then enter a new password from that DN.

To create or reset a call log password:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Click on the **General** heading.
4. Type a 4-digit password in the **Call log passwords** box, or leave it blank, and press **Enter**.

Line access

Line access allows you to assign lines to individual telephones. To save time, you can copy the Line access settings to other telephones once you have finished programming the settings for one telephone.

Note: PRI lines must be set to Auto Answer; they cannot be Manual Answer.

Tips

When you assign line access for BRI loops make sure that the programming for the two lines on a BRI loop is identical. For example, if line 001 on BRI loop 201 appears at a DN, line 002 on the same loop should appear at the DN as well.

In general, you do not assign, auto-answer loop start trunks and auto-answer BRI trunks to telephones. If assigned, they are for monitoring incoming call usage, or for making outgoing calls.

To assign a line to a telephone:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**, **DN**. Click on the **Line access** heading.

2. Configure line access according to the table:

Attribute	Description
Prime line	You can define the first line that a telephone selects when you make a call from an Enterprise Edge telephone. PRI pools are not valid selections for a Prime line. Note: An assigned prime line is not associated with the assignment of a prime telephone. Values: **None**, **Pool** (**A** to **O**), **I/C** (intercom), or **Line:** (Default: **None**)
Intercom keys	You can assign the number of intercom buttons to a telephone. Intercom buttons provide a telephone with access to internal and external lines, and line pools. Refer to Intercom keys on page 94. Values: **0** to **8** (Default: **2**)
OLI number	You can define the digits used for originating line identification number (OLI). Refer to OLI number on page 95. Values: up to 24 digits (Default: **blank**)

You must assign an external line to the telephone in **Line assignment** (see Line assignment on page 95) before you can assign the line as the prime line to the telephone. You must assign a line pool to the telephone in **Line pool access** (see Line pool access on page 97) before you can assign a line pool as the prime line to the telephone. A target line cannot be a prime line for a telephone because it is incoming-only.

Note: Do not assign a T1 DID line as the prime line for a telephone. If assigned, the system treats it as if there is no prime line. The set displays the message **Select a line** when you lift the receiver.

When you assign a line pool as a prime line, the system searches automatically for an idle line in the pool. For more information, see Line type on page 116.

3. Choose the Prime line for this DN (**Line 001**, **Pool A**, **None**, **I/C**). The default is **I/C**.

Intercom keys

The Intercom keys attribute assigns the number of intercom keys. Intercom keys provide a telephone with access to internal and external lines, and line pools.

When you assign each Intercom key during programming, it automatically appears on the telephone. The intercom keys appear on the lower-right button, or one key above if the Handsfree/Mute feature appears on the telephone.

When you assign the number of Intercom keys:

- A telephone requires two intercom buttons to be able to establish a conference call with two other Enterprise Edge telephones.
- You require only one intercom button if the button is used to make and receive internal calls, and to access line pools. You require two intercom keys for a telephone with several lines assigned to Ring only.
- The M7100 telephone can have up to eight intercom buttons although the telephone has one programmable button.

4. Choose the number of Intercom keys you want to assign to this DN (**0**, **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**). The default is **2**.

OLI number

The originating line identification number (OLI) setting allows you to specify the number that displays on the telephone you are calling.

Enter the digits used for the originating line identification number (OLI).When you make an outgoing call on a BRI line, the Call Display information that appears on the telephone you are calling is usually based on the first Network DN associated with the line.

If the line has more than one Network DN, you can program a DN to use a Network DN other than the first one for the outgoing Call Display information. When you program the alternate Network DN as the ten-digit outgoing line identification (OLI) number, and you make a call using the line associated with the Network DN, the OLI number appears on the telephone you are calling.

If an outgoing call is made using a line that is not associated with the Network DN number used as the OLI number, the network ignores the number; the default Call Display information (the first or only Network DN associated with the line) appears.

5. Enter the **OLI number** in the box. The default is blank. OLI numbers for North America are ten digits.

Line assignment

The Line assignment setting allows you to assign physical trunks and target lines to each telephone. You can assign and remove target lines the same as other lines. You can also assign multiple target lines across a group of sets in a Broadcast ring group.

To assign a trunk or target line to a telephone:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528) that you want to assign to a trunk or line.

3. Choose **Line access**. Click on the **Line assignment** heading.

4. Click the **Add** button above the navigation tree.

5. Type a line number in the **Line** box.

6. Click the **Save** button.

7. Click on the **Line nnn** you just created.

Appearance type

Select how a call on this line shows at the set.

8. In the DN nnn-Line nnn window, choose the line Appearance type. **Ring only**, **Appear&Ring**, or **Appear only**. The default is Unassigned.

Note: Enterprise Edge will not support a mixture of **Appear only** and **Ring only** appearances for the same line. If you choose **Appear&Ring** or **Appear only**, you can have as many simultaneous DID calls as there are target line key appearances. If you choose **Ring only**, you can have as many simultaneous DID calls as you have intercom keys.

Call log set

The Call log set attribute allows you to specify if the telephone automatically logs Call Display information for calls on an external line. The line must appear on that telephone, but it does not have to be a ringing line.

9. Click **Y** or **N** to enable call logging. The default is **N**.

Vmsg (Voice Message) set

If you subscribe to an external voice message service, you can access that service through your Enterprise Edge system. The voice message setting controls if the indicator shows on a telephone for voice message waiting on a particular line. The line must appear on that telephone.

10. Click **Y** or **N** to enable voice message waiting indicator. The default is **N**.

To find out if your voice message service works with Enterprise Edge, or if you have any problems with your service, contact your voice message service provider.

PRI Lines

Users cannot access PRI lines directly through line appearances or line pools. To dial outgoing PRI calls use the intercom button and enter a routing code.

When an EE-DTM changes to PRI, the system automatically removes all existing line appearances for that module.

The Enterprise Edge Analog Terminal Adapter (ATA 2), BRI S-terminals, or a portable cannot process more than 2 simultaneous calls.

There is a suggested limit of 4 keys per set. You can program more than 4 keys on a set by programming less than 4 on other sets. For instance, you might program 20 keys on a receptionist set equipped with a CAP.

Tips

In general, you do not assign auto-answer loop start trunks, auto-answer T1 E&M trunks and T1 DID trunks to telephones. If assigned, they are used for monitoring incoming call usage, or for making outgoing calls (auto-answer loop start and T1 E&M trunks).

You cannot assign a line that is private to another telephone.

Each line assigned to appear at a telephone must appear at a button with an indicator on that telephone. The maximum number of line buttons is 8 for the M7208 telephone, 10 for the M7310 telephone, and 24 for the M7324 telephone.

If you set a line to Ring only, incoming calls appear on an intercom button.

A central answering position (CAP), with one or two CAP modules, can provide extra line buttons if more than 24 lines are assigned to the CAP. The remaining lines appear at buttons on the CAP module.

The M7100 telephone is an exception; it has no line buttons and can be assigned any number of lines. Make sure that lines assigned to an M7100 telephone are assigned to ring; otherwise, you cannot detect incoming calls on the lines.

Line pool access

The Line pool access setting allows a telephone to access one or more of the fifteen line pools available (A to O). Six exclusive line pools (PRI-A to PRI-F) are available for PRI lines. Only three are currently supported.

Only PRI or BRI-QSIG lines can belong to a PRI pool. PRI lines cannot belong to Line Pools A through O, and all lines on a single EE-DTM (PRI) belong to the same pool. Lines from multiple EE-DTM (PRI) can belong to the same pool if they are configured with the same protocol. You can assign PRI lines to pools with the **Line type** setting.

To assign a line pool to a telephone:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Line access**, **Line pool access.**
4. Click the **Add** button above the navigation tree.
5. Enter a letter from **A** to **O**.

6. Click the **Save** button.
   The set can now access any line in that line pool.

Answer DNs

You can program a telephone to provide call alerting and call answering for other telephones. The DNs of the other telephones are referred to as Answer DNs.

Every Answer DN you assign to the telephone automatically designates an Answer button with an indicator to the telephone. Label the buttons to identify the telephone with its name or DN. More than one telephone can have an Answer button for the same DN.

You can assign a maximum number of eight Answer DNs to a set.

To create an answer DN on a telephone:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Line access**. Click on the **Answer DNs** heading.
4. Click the **Add** button above the navigation tree.
5. Type the Answer DN.
6. Click the **Save** button.

Answer type

1. Select the newly created Answer **DN**.
2. Choose the Answer type: **Appr&Ring**, or **Appr only**. The default is **Appr&Ring**.

Capabilities

The Capabilities settings control how the system interacts with individual telephones and how they receive calls.

To define telephone capabilities:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Click on the **Capabilities** heading.

4. Configure Capabilities settings according to the table:

Attribute	Description
DND on busy	Defines whether an incoming call rings if you are already on another call. Values: **Y** or **N** (Default: **N**)
Handsfree	Defines whether Handsfree is available to a telephone. Values: **Auto**, **Standard**, **None** (Default: **None**)
HF answerback	Defines whether you can automatically answer a voice call without lifting the receiver or pressing the Handsfree/Mute button. Values: **Y** or **N** (Default: **Y**)
Pickup group	Assigns this telephone to a pickup group. Values: **None**, **1** to **9** (Default: **None**)
Page zone	Assign this telephone to page zone. Values: **None**, **1** to **6** (Default: **1**)
Paging	Defines whether you can make paging announcements from this telephone. Values: **Y** or **N** (Default: **Y**)
Direct dial	Defines whether you can call the Direct-dial telephone from this telephone using the Direct-dial digit. Values: **Set 1** to **Set 5**, **None** (Default: **Set 1**)
Priority call	Defines whether this telephone can interrupt calls or override Do Not Disturb at another telephone. Values: **Y** or **N** (Default: **N**)
Aux ringer	Defines whether an auxiliary ringer (if installed) rings for incoming calls at this telephone. Values: **Y** or **N** (Default: **N**)
Allow redirect	Defines whether this telephone can redirect its lines. Values: **Y** or **N** (Default: **N**)
Redirect ring	Defines whether the telephone rings briefly when a call on one of its lines is redirected by the Line Redirection feature (Feature 8 4). Values: **Y** or **N** (Default: **Y**)

Call forward

The Call forward setting allows you to define how unanswered calls are handled or when the line is busy.

To program call forward:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528).

3. Choose **Capabilities**, click on the **Call forward** heading.

4. Configure Call Forward according to the table:

Attribute	Description
Fwd no answer to	You can redirect all incoming calls when this telephone does not answer. Values: up to **24** digits (Default: **blank**)
Fwd no answer delay[1]	You can define the number of rings before the system forwards an unanswered call. Values: **2**, **3**, **4**, **6**, **10** (Default: **4**)
Fwd on busy to	You can redirect all incoming calls when this telephone is busy with another call. Values: up to **24** digits (Default: **blank**)
Notes: 1 Appears after you have entered a call forward no answer number and pressed Enter.	

Hotline

The Hotline setting allows you to define a telephone number that automatically dials when you lift the receiver or press the Handsfree/Mute button on a set. You can define an internal or external number.

To define an internal Hotline telephone number:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities**. Click on the **Hotline** heading.
4. Click **Internal,** and then press **Enter**.
5. In the **Internal #** box, choose Direct dial set or DN:, and then type the DN number (up to 3 digits).

To define an external number as a hotline:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities**. Click on the **Hotline** heading.
4. Click **External**.
5. In the **External #** box, type the telephone number (up to 24 digits).

6. Click a Facility value: **Use line nnn**, **Use prime line**, **Pool code**, **Use routing table**.

   Note: For Pool, type a letter from A to O and then press Enter. For Use line, type a number from 001 to 238, and then press Enter. You cannot use Target lines as the facility.

ATA settings

The ATA settings allow you to define general settings for analog terminal adapters.

To configure ATA settings:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities**. Click on the **ATA settings** heading.
4. Configure ATA settings according to the table:

Attribute	Description
ATA answer timer	Select the length of delay between the last digit you dial and when the Enterprise Edge ATA 2 device is ready to receive DTMF tone. Values: **3**, **5**, **7**, **10** (Default: **7**)
ATA use	Select the location of the Enterprise Edge ATA 2. Values: **On site**, **Off site** (Default: **Off site**)
Msg Indicate	Select the type of message indicator. Tone sends a Message Tone through the set's receiver and Lamp turns on the set's Message Lamp when you receive a message. Values: **None**, **Tone**, **Lamp** (Default: **None**)

Tips

If you have a modem or fax machine keep the ATA answer timer delay short. If a call to a fax machine or modem cannot connect, try shortening the delay. If an individual is dialing the number for a fax machine or modem, you may want to make the delay a little longer.

User preferences

The User preferences settings allow you to do the same programming that users can do at their telephones. If the attached set is not an Enterprise Edge set, these options are not available.

To configure User preferences settings:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528).

3. Click on the **User preferences** heading.

4. Configure User preferences settings according to the table:

Setting	Description
Model	Pre-program the model of Enterprise Edge set that will use this DN (M7310). You cannot change the model if the set is already attached.
Call log options	Select whether the set will: **Log all calls**, **No autologging**, **No one answered** or **Unanswered by me**.
Dialing options	Select **Standard dial**, **Pre-dial** or **Automatic dial**.
Language	Choose the display language: **English**, **French** or **Spanish**.
Contrast	Adjust the contrast of the display **1**, **2**, **3**,**4**, **5**.....**9**
Ring type	Select a ring type **1**, **2**, **3**, **4**

Button programming

The Button programming heading allows you to program the telephone buttons with internal and external autodialers and programmed feature keys.

1. Click on the key to expand the **User preferences** heading.

2. Click on the **Button programming** heading.
   The list of available buttons expands.

3. Click on the button you want to program.

4. In the **Type** box, choose **External autodial**, **Feature**, **Blank**, or **Internal autodial**.

5. Press **Enter** to refresh the screen.

External autodial

The **Value** and **External #** boxes appear.

6. In the **Value** box, choose the line for the external autodial.

7. In the **External #** box, type the telephone number.

Feature

The **Value** box appears.

8. In the **Value** box, choose the Feature code you want to program on this button.

Internal autodial

The **Value** and **Internal #** boxes appear.

9. In the **Value** box, choose the line for the internal autodial.

10. In the **Internal #** box, type the DN.

User speed dials

1. Click on the key to expand the **User preferences** heading.

2. Click on the **User speed dials** heading.

3. Click the **Add** button above the navigation tree.
   The Add User speed dials screen appears.

4. In the **Speed dial #** box, type in the internal or external telephone number.

Restrictions

The Restrictions settings prevent you from making certain kinds of calls from a telephone or from lines that are available at the telephone. You can also restrict some features.

When you finish programming restriction settings for one telephone, you can copy those settings to other telephones.

To configure Restrictions settings:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528).

3. Choose **Restrictions**. Click on the **Set restrictions** heading.

Set restrictions

The Set restrictions window Allows you to assign a restriction filter to a telephone to prevent certain numbers from being dialed from that telephone, and prevent the use of certain features.

Set lock

You can adjust the amount of personal programming and customizing that can be done at a telephone.

4. Select the setting: **None**, **Partial**, or **Full**.

None allows you access to all features on your telephone.

Partial prevents:

- programming autodial buttons
- programming user speed dial numbers
- programming feature buttons
- moving line buttons
- changing the display language
- changing dialing modes (Automatic Dial, Pre-Dial, and Standard Dial)
- using Voice Call Deny
- saving a number with Saved Number Redial

Full, in addition to the restrictions outlined for Partial lock, prevents:

- changing Background Music
- changing Privacy
- changing Do Not Disturb
- using Ring Again
- using Call Forward all calls
- using Send Message
- using Trunk Answer
- activating Services

Allow last number

5. Click **Y** or **N** to allow a set to use the Last Number Redial feature.

Allow saved number

6. Click **Y** or **N** to allow a set to use the Saved Number Redial feature.

Allow link

7. Click **Y** or **N** to allow a set to use the Link feature (a host signaling option).

Schedules

You can assign a different restriction filter for normal service and for each of six schedules. See Scheduled Services on page 138 for more information about the schedules.

To configure Restrictions Schedules settings:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528).

3. Choose **Restrictions, Set restrictions, Schedules**.

4. Click on the schedule you want to program. For example, **Evening**.

5. In the **Use filter** box, type in the number of the restriction filter you want to assign to the set.

Schedule	Restriction filter
Normal	02
Schedule 1 (Night)	11
Schedule 2 (Evening)	12
Schedule 3 (Lunch)	13
Schedule 4	00
Schedule 5	00
Schedule 6	00

For example, if you enter a set of restrictions for filter 11, the restrictions will automatically apply for the Night schedule.

Line/set restrictions

The Line/set restrictions attributes allows you to assign a restriction filter to a specific line for outgoing calls at a specific telephone. This type of filter replaces any line or set restriction filters that might otherwise apply. The Line/set restrictions restricts the numbers you can dial on a line, but only from that telephone. The same line on another telephone can have different restrictions.

As with set restrictions, you can apply a different line restriction for normal service and for each of six schedules.

To configure Line/set restrictions settings:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528).

3. Choose **Restrictions, Line/set restrictions.**

4. Click on the **Line** number you want to configure.
   The list of schedules expands on the navigation tree.

5. Click on the schedule name that you want to configure. For example, **Night**.
   The Night schedule window appears.

6. In the **Use filter** box, choose **None** or **Filter:**. Type the number you want to assign as the line/set restriction for this schedule and press the **Enter** key.There are no default line/set restrictions.

Tips

A maximum of 255 line/set restrictions may be applied to lines at telephones.

If you assign a line/set restriction to a line at a particular telephone, it overrides any line restrictions or set restrictions that might otherwise apply.

If no line/set restrictions are defined, the numbers are checked against the set restrictions and the line restrictions, if either of these have been defined. The numbers may be rejected by either restriction.

Telco features

The Telco features settings program the way Enterprise Edge works with public network or other outside features and services. Enterprise Edge works with two of these services: Call Display and an external voice message service.

When you finished programming Telco features settings for one telephone, you can copy those settings to other telephones.

To configure Telco features settings:

1. Choose **Services**, **Telephony Services**, **Terminals & sets**.

2. Click the telephone set (DN 221-528).

3. Choose **Telco features**.

Feature assignment

If you subscribe to Call Display services (often called Caller ID), external calls are identified on the display. You may also have a message indicator from an external voice mail service show on the set's display. Analog Call Display services are available with an EE-CTM. You can customize how this information is used.

PRI also provides the Caller ID.

4. Select the number of the line you want to program with Feature settings.

First display

Depending on the services you subscribe to, Call Display information may contain the number of the caller, the name of the line in your Enterprise Edge system that the call is on, or both. For each telephone, you can determine what information displays first.

5. Select the setting: **Name**, **Number** or **Line**.

Tips

The Call Information feature displays and toggles between the name and line number for Call Display information.

You may see **Unknown number** on the display if the information is not available from your telephone company. You may see **Private number** on the display if the caller blocks that information.

Auto called ID

The Auto called ID setting allows you to see the extension number and name on your display, of the set you call. The Auto called ID set for target lines is the same set that has appearance on that target line.

6. Click **Y** or **N** to enable Auto called ID.

Set log space

The Log space settings determines the number of items that can be stored in the Call log for each telephone. There is no log space assigned by default.

7. Enter an amount. **Available log space** indicates the amount of space remaining.

Tips

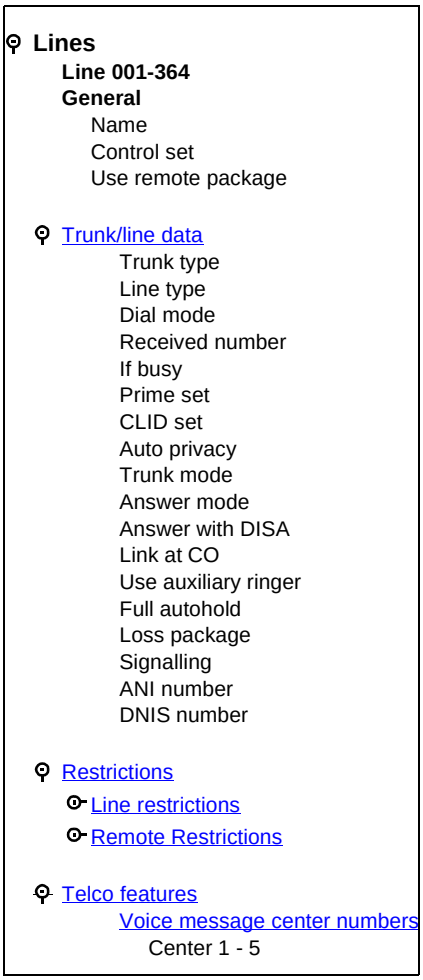
There must be space available in the log pool in order for you to add space to a Call log. The maximum number of spaces available is 600.

You can allocate system-wide log space in Call log space under **General settings**. If you want to allocate the same log space to all telephones, use the Call log space setting instead.

Lines

The Lines heading allows you to assign attributes for each line. The following illustration shows a detailed view of the Lines programming map.

Note: Lines 001 to 014 are for VoIP trunks. Lines 241 to 364 for target lines.



To program settings for a line, click the line number (Line 001-364) of the line and click the key beside the selected line number to display the programming sublevels.

Copying settings from one line to another

The Copy commands allows you to duplicate programming for a line and apply it to another line or a range of lines.

When you copy data from a physical trunk to a target line (or the other way around), only the data in common is copied. For example, copying a target line to a T1 E&M trunk copies only the Line data settings because there are no Trunk data settings for a target line.

Note: You cannot copy programming between lines on different types of modules. The Received number of a target line is a unique number and cannot be copied.

To copy line settings:

1. Choose **Services, Telephony Services, Lines**.
2. Click the line (Line 001-364) from which you want to copy settings. If necessary, choose a subheading to refine your selection.
3. On the **Edit** menu, click **Copy**.
4. Click **Single** or **Range** from the Copy type list.
5. In the **Copy to** box, type the line number or the start and end line numbers of the range of lines where you want to copy the settings.
6. Click the **OK** button.

General

The General heading allows you to assign the name, a control set, and a remote package for a line.

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Choose the line number (Line 001- Line 364).
3. Click **General**.

Name

The default name for a line is “Line” and its three-digit number (for example, Line 001), but you can change it to any combination of letters and numbers to a maximum length of seven characters.

To change the name of a line:

4. In the **Name** box, type a name (up to seven characters) and then press **Enter**.

Control set

The Control set attribute allows you to define a DN that acts as a control set for a line. By default, DN 221 is the control set for all lines. A control set turns Scheduled Services on and off for the lines assigned to it. For more information about services, see Scheduled Services on page 138.

You can assign several control sets for your system but you can only assign one control set per line.

Tips

External lines and telephones must be programmed with a control set to use the three kinds of Scheduled Services: Ringing, Restriction, and Routing Services.

One recommendation is to have one control set for all lines and a different control set for all telephones.

You can turn on a service manually or automatically for all external lines controlled by a given control set, but you cannot combine schedules. In other words, a service can only be active as normal service or one of the six schedules at any one time. You can have several schedules active, as long as they are using different services.

5. In the **Control set** box, type the DN number and press Enter, or click **None**.

Use remote package

The Use remote package attribute allows you to define whether remote users can access line pools or not. The table below shows the remote package settings. Remote package 00 is the default setting for the Use remote package setting. It permits no access to line pools. Unlike packages 01 to 15, you cannot change package 00. You can define up to 15 remote access packages (01 to 15). You can also copy settings from one remote package to another.

Parameter	PBX DID
Package 00	Prohibits remote access to line pools, Page, remote monitoring and administration. Cannot be changed.
Package 01 Line pool access	**Y for Pool A** **N for Pools B to O and PRI-A to PRI-F**
Packages 02 - 15 Line pool access	**N for Pools A to O and PRI-A to PRI-F**

To assign a remote package:

6. In the **Use remote package** box, type the two-digit remote package number, and then press **Enter**.

Tips

The line pool access display shows an alphabetic line pool identifier, followed by a numeric line pool access code in brackets, for example, **Pool A (9):N**. If no access code has been identified, there is nothing between the brackets, for example **Pool A ( ):N**. The line pool access code can be programmed under **Terminals & sets**.

Trunk/line data

The Trunk/line data attributes allow you to program settings for lines that affect how Enterprise Edge communicates with other switches, and allows you to determine how lines (including target lines) are used in Enterprise Edge.

To configure a trunk or line:

1. Choose **Services, Telephony Services, Lines, Line nnn**.

2. Click on the **Trunk/line data** heading.

3. If you have a T1 module, select a trunk type: **Loop**, **E&M**, **DID**, **Ground**, or **Fixed data channel**.

   Any other module shows the trunk type but you cannot change this setting. For more information about trunk types, see Trunk type on page 115.

   Note: You can only change the trunk type setting for lines connected to an T1 module. All other lines are automatically configured based on the type of hardware module present. VoIP is automatically assigned as the trunk type to Lines 001 to 014 and cannot be changed.

   Trunk/line data settings vary depending on the type of trunk that has been programmed and the hardware to which the trunk is connected. The following table lists the options that are available for each trunk type. A checkmark indicates that the option is present.

	Trunk type										
	Loop start Analog	Loop start Digital	Ground start Digital	DID Digital	E&M Digital	BRI-ST	PRI lines	Target lines	VoIP	DASS2	DPNSS
Line type	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Dial mode	✓	✓	✓	✓	✓	—	–	–	–	–	–
Received #	–	–	–	–	–	—	–	✓	–	✓	–
If busy	–	–	–	–	–	—	–	✓	–	✓	–
Prime set	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CLID set	✓	✓	–	–	✓	✓	–	✓	–	✓	✓
Auto privacy	✓	✓	✓	✓	✓	✓	–	–	✓	–	✓
Trunk mode	✓	✓	–	–	–	—	–	–	–	–	–
Answer mode	✓	✓	✓	–	✓	✓	–	–	–	–	✓
Answer with DISA	✓	✓	✓	–	✓	✓	–	–	–	–	–
Link at CO	✓	–	–	–	–	—	–	–	–	–	–

	Trunk type										
	Loop start Analog	Loop start Digital	Ground start Digital	DID Digital	E&M Digital	BRI-ST	PRI lines	Target lines	VoIP	DASS2	DPNSS
Use auxiliary ringer	✓	✓	✓	✓	✓	✓	–	✓	✓	✓	✓
Full autohold	✓	✓	–	–	–	✓	–	–	✓	–	✓
Loss package	✓	–	–	–	–	—	–	–	–	–	–
Signal	–	–	–	✓	✓	—	–	–	–	–	–
ANI Number	–	–	–	✓	✓	—	–	–	–	–	–
DNIS Number	–	–	–	–	✓	—	–	–	–	–	–

4. Configure the line settings according to the following table (again, available option fields will depend on the line type selected):

Attribute	Description
Line type	Define how the line is used in relation to other lines in the system. • A Public line can be accessed by more than one telephone. • A Private line can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool assigns the line to one of the 15 line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. Values: **Public**, **Private to:**, **Pool A** to **O**, **PRI-A** to **PRI-F** (Default): **Public** For more information and Tips, refer to Line type on page 116.
Dial mode	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signalling on the trunk. Tone does not appear if Signalling is set to Immediate (T1 DID &T1 E&M trunk types only). Values: **Pulse**, **Tone** (Default: **Tone**)
If busy	Define whether a caller gets a busy tone or the call forwards to the prime set when the target line is busy. Busy tone only works for PRI trunks. Values: **To Prime**, **Busy Tone**

Attribute	Description
Prime set	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls will be redirected if the received number is invalid or the target line is busy, and if the 'If busy' parameter is set '**To prime**'. Each line can be assigned only one prime set. Values: **DN:**, **None** (Default: **DN 221**)
CLID set	Specify what sets are capable of using the Call Line Identifier (CLID) feature. Values: **DN:**, **None** (Default: **None**)
Auto privacy	Define whether one Enterprise Edge user can select a line in use at another telephone to join an existing call. ***Tips*** Users can change a line's privacy setting for an individual call using the Privacy feature (Feature 8 3). Values: **Y** or **N** (Default: **Y**)
Trunk mode	Define whether disconnect supervision, also referred to as loop supervision, releases an external line when an open switch interval (OSI) is detected during a call on that line. You must set this to Supervised if a loop trunk has its Answer mode set to Auto or if you enable Answer with DISA. Disconnect supervision is also required to conference two external callers. The line must be equipped with disconnect supervision from the central office for the Supervised option to work. ***Tips*** The duration of an open switch interval (OSI) before Enterprise Edge disconnects a call is programmed by the **Disconnect timer** setting. See Hardware on page 84 for more information. Values: **Unspr**, **Supervised** (Default: **Unspr**)
Answer mode	Define whether a trunk is manual or automatic answer. The Answer mode setting appears for T1 ground start lines, T1 E&M lines, and T1 loop start lines and BRI lines whose Trunk mode setting is set to Super. Select the setting: **Manual** or **Auto**. **Note:** You require Disconnect supervision if loop start trunks are to operate in auto-answer mode. Values: **Manual**, **Auto** (Default: **Manual**)
Answer with DISA	Define whether the system prompts a caller for a six digit class of service (COS) password. This setting appears for T1 loop start and T1 E&M lines that have auto-answer mode. Set this option to No for T1 E&M lines on a private network that have auto-answer mode. Values: **Y** or **N** (Default: **Y**) To program DISA on a PRI trunk, see Direct inward system access (DISA) on page 331.

Attribute	Description
Link at CO	Some exchanges respond to a Link signal (Feature 7 1) by providing an alternative line for making outgoing calls. When you enable Link at CO, the system applies the restrictions on outgoing calls to the digits dialed after the Link signal, and the call on the alternative line is subject to all restrictions. Disabling Link at CO prevents a Link signal from resetting the Enterprise Edge restrictions in cases where the host exchange does not provide an alternative line. Values: **Y** or **N** (Default: **N**)
Use auxiliary ringer	Allows you to turn the auxiliary ringer on or off. Refer to Use auxiliary ringer on page 117. Values: **Y** or **N** (Default: **N**)
Full autohold	Enables or disables full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. Applies to loop start and VoIP trunks. Full autohold is always in place for T1 E&M trunks; it has no meaning for incoming-only T1 DID trunks. The default setting should be changed only if Full autohold is required for a specific application. Values: **Y** or **N** (Default: **N**)
Loss package	Allows you to select the appropriate loss/gain and impedance settings for each line. For more information refer to Loss package on page 117. Values: **Short CO**, **Medium CO**, **Long CO**, **Short PBX**, **Long PBX** (Default: **Medium CO**)
Signalling	Defines the signal type for the line. Applies to T1 E&M or T1 DID trunks. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to an EE-DTM if the Dial mode is set to tone. Make sure that this matches the signal type programmed for the trunk at the other switch. Values: **WinkStart**, **Immediate**, **DelayDial** (Default: **Winkstart**)
ANI Number	Defines whether the telephone number of the caller will be collected for this line. Applies to T1 E&M and T1 DID trunks. For T1 E&M and T1 DID trunks connected to an EE-DTM, this setting only appears if Signalling is set to WinkStart. The central office must deliver ANI/DNIS in DTMF mode. No additional equipment is required. Values: **Y** or N (Default: **N**)
DNIS Number	Defines whether the digits dialed by an external caller on this line will be collected. Applies to T1 E&M trunks. For T1 E&M trunks connected to an EE-DTM, this setting only appears if Signalling is set to WinkStart and Answer mode is set to Manual. These digits are required for some third-party software applications. Values: **Y** or **N** (Default: **N**)

Trunk type

Trunk/line data varies with the type of trunk module, the configuration, and what line you select. For example, you can configure the EE-DTM as PRI or T1.

You can program the following trunk types:

Hardware Unit	Trunk Types
EE-DTM	PRI T1 Loop, T1 E&M, T1 Ground, T1 DID, T1 Fixed DASS2 DPNSS
EE-CTM (North America)	Loop
EE-BRIM S/T	BRI-S/T

Note: The Fixed data channel trunk type is required if you want to use the soft router feature in Enterprise Edge. You must first install an EE-DTM and configure it as Module type, T1 (see Module on page 72.) You must then configure the Trunk type as Fixed data channel. You can now configure Module 08 as a Data module (see Configuring a data module on page 79).

Enable modules

If you disabled any Trunk Modules prior to perform programming, enable them now, or your system will not function properly. See Media Bay Module status on page 279.

Voice over IP trunk considerations

For IP functionality with Enterprise Edge VoIP Gateway, the trunk type is **VoIP.** Enterprise Edge VoIP Gateway routes voice traffic over private Internet Protocol (IP) networks to link multiple sites together using an existing corporate data network. Lines 001 to 014 are reserved for IP functionality. The number of lines available for use is a function of software key codes and currently eight of the 14 lines are available for IP functionality.

Note: VoIP trunks should not be accessed through Line appearances as the user will not receive dial tone.

VoIP trunks should be configured to use a discrete line pool (Pool A to O). Do not mix other trunk types on the same line pool. You can configure your IP trunks to use the fallback feature.The use of Line pool codes is not recommended as you will not be able to configure for fallback. The quality of the IP trunk connection is assessed during initial call setup, and if the quality is outside the configured threshold, Enterprise Edge will try to find an alternate route to complete the call (fallback) based on the programming definitions in the routing table. If you do not configure your network for fallback and the call quality is below threshold, the IP call will fail. For an example of a network configuration that supports fallback, see Toll bypass with Enterprise Edge VoIP Gateway on page 351.

When fallback is configured, the IP call will be rerouted to a circuit-switched connection. This could be either a private network trunk or it could be a public network trunk. Ideally you would want to configure fallback to use the least cost route if possible. For more information about configuring VoIP trunks, see the *Enterprise Edge IP Telephony Configuration Guide*.

Line type

Tips

Line pools must never contain a mixture of lines. All lines in a given line pool should go to the same location.

Try to avoid putting unsupervised loopstart lines in a line pool. These lines can become hung, especially when a remote user uses the line pool to make an external call.

There are two more programming settings that must be assigned before a line pool can be used:

- You must assign line pool access to telephones in **Line access** programming.
- You must assign system-wide line pool access codes in **General settings** (not applicable to PRI pools).

Tips

A telephone can be administered to search automatically for an idle line from several lines appearing on the telephone. Assign a line pool as the prime line (in **Line access**) and all the lines in the line pool must appear on that telephone. When the user lifts the receiver or presses Handsfree/Mute, any one of the lines, if idle, can be selected by Automatic Outgoing Line selection.

Changing the settings for trunk type on a system that is in use may cause calls to be dropped.

When assigning lines to line pools, consider your network configuration. You may be able to create a unified dialing plan by assigning lines to the same location to the same line pool on each of your systems. For example, if system A and system B each have tie lines to system C, assign the tie lines to pool D on each of the systems.

You cannot assign target lines to a line pool.

Use auxiliary ringer

This setting allows you to turn the auxiliary ringer on or off. An auxiliary ringer can be programmed on a line or a set. When programmed on a line, the auxiliary ringer will ring every time a call is received. When programmed only on a set, the auxiliary ringer will not ring when a transferred call is received.

Tips

The auxiliary ringer is an optional device that should be connected by the installer.

If you have an auxiliary ringer programmed to ring for calls on an external line, and you transfer a call on that line without announcing the transfer, the auxiliary ringer will ring for the call transfer.

An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service.

Loss package

Loss package allows you to select the appropriate loss/gain and impedance settings for each line. The setting is based on the distance between Enterprise Edge and the terminating switch, and the terminating switch type. When measuring the distance from Enterprise Edge to CO and from Enterprise Edge to PBX, use 600 ohms as the termination resistance setting.

Loss Package	Receive Loss	Transmit Loss	Impedance	Distance to switch/cable loss/terminating switch
Short CO	0 dB	3 dB	Short	Short/<2 dB/Enterprise Edge to CO
Medium CO	0 dB	0 dB	TIA/EIA 464	Medium/>2 dB and <6 dB/ Enterprise Edge to CO
Long CO	-3 dB	0 dB	TIA/EIA 464	Long/>6 dB/Enterprise Edge to CO
Short PBX	0 dB	0 dB	Short	Short/<2 dB/Enterprise Edge to PBX
Long PBX	-3 dB	0 dB	TIA/EIA 464	Long/>2 dB/Enterprise Edge to PBX

A loss of 4 dB corresponds to a cable length of approximately 2700 m (9000 ft).

Setting Received number

The Received number attribute allows you to specify the digits to make a specific target line ring. A received number cannot be the same as, or be the start digits of a line pool access code, a destination code, the DISA DN or the Auto DN.

If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. The call will be directed to the prime telephone for the incoming line if the Network DN is not used.

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**, **Trunk/line data** and click on the **Received number** heading.
   The Received number screen for the line appears.

2. Type in the Received number in the **Public number** box (for North America). or type in the **Public number** and **Private number** (for UK). The default is blank.

Restrictions

Restrictions prevent you from making certain kinds of calls from specific lines on the telephone. You can also restrict some features. This section describes how to apply restriction filters to lines; see Restriction filters on page 124 for details on creating the filters.

Line restrictions

The Line restrictions attribute allows you to specify the filter applied to this line to restrict the dial out numbers. You can assign a different restriction filter for normal service and for each of six schedules. See the section on Services for more information about the schedules. For PRI, line restriction changes apply to all 23 lines.

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**, **Restrictions**, **Line restrictions**.

2. Click on the schedule heading that you want to configure. For example, **Night**.
   The Line restriction window for that schedule appears.

3. In the **Use filter** box, type in the number of the restriction filter you want to assign as the line restriction for this schedule. The default restriction filters are as follows:

Schedule	Restriction filter
Normal	03
Schedule 1 (Night)	21
Schedule 2 (Evening)	22
Schedule 3 (Lunch)	23
Schedule 4	00
Schedule 5	00
Schedule 6	00

Tips
When a remote user places an external call on a line, any filters used with the line still apply.

Remote Restrictions

Specify the restriction filter for the line that remote callers use to call in to Enterprise Edge. A restriction filter is a set or group of restrictions and overrides. As with line restrictions, you can apply a different remote restriction for normal service and for each of the six schedules.

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**, **Restrictions**, **Remote restrictions**.

2. Click on the schedule heading that you want to configure. For example, **Night**.
   The Remote restriction window for that schedule appears.

3. In the **Use filter** box, type in the number of the restriction filter you want to assign as the remote restriction for this schedule.

Select the remote restrictions for each schedule. The default restrictions are as follows:

Schedule	Restriction filter
Normal	04
Schedule 1 (Night)	31
Schedule 2 (Evening)	32
Schedule 3 (Lunch)	33
Schedule 4	00
Schedule 5	00
Schedule 6	00

Tips

The remote restriction restricts the numbers that can be dialed on an incoming auto-answer line. If a remote user then selects a line to place an external call, any filter used with the line still applies.

Telco features

If you subscribe to a voice message service outside your office, you can access it through your Enterprise Edge system. You can specify what voice message center you use for each external line that receives message waiting indication.

1. Choose **Services**, **Telephony Services**, **Lines**, **Line nnn**.

2. Click on the **Telco features** heading.
   The Telco features window for the line appears.

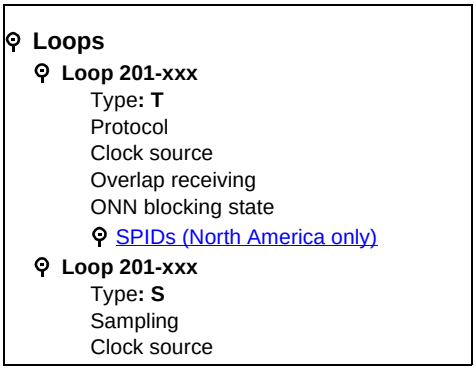
3. Select the Voice message center for the line, **Center 1** - **Center 5** or **None**.

Note: To program the external numbers for each Center, refer to Voice message center numbers on page 187.

Loops

The Loops heading allows you to program BRI loop settings.

The following illustration shows a detailed view of the Loops programming map.



Note: Headings will vary according to your market profile.

Configuring the loop type

The Media Bay Modules support two types of BRI loops: S and T.

To configure a T loop:

1. Choose **Services**, **Telephony Services**, **Loops**.
2. Select a loop number (for example, Loop 201).
3. Set the Type to T.
4. Configure the loop settings according to the table:

Attribute	Description
Protocol[1]	Allows you to select the appropriate ISDN protocol. The values displayed depend on both the market profile and software keycodes. NI is National ISDN. Euro is the ETSI ISDN standard. Q-Sig is also an ETSI standard and appears if the Q-Sig software key is loaded. Values: **Euro**, **Q-Sig**
Clock source	Allows you to designate a clock source for maintaining system synchronization. Values: **Master**, **Primary**, **Secondary** (Default: **Master**)
Overlap receiving	Allows for support of target lines in markets which use Overlap receiving signalling on the BRI trunks. Overlap receiving must be configured for each BRI loop. Values: **Y** or **N** (Default: **N**)
Local number length	Allows you to set the local number length. This parameter appears only when Overlap receiving is set to Y. Values: **0**-**10** (Default: **8**)

Attribute	Description
ONN blocking state	Allows you to set the ONN block state. Values: **Suppression bit**, **Service code** (Default: **Suppression bit**)
Notes: 1 The values displayed depend on the market profile that is loaded. Euro and Q-Sig appear in all the European profiles.	

To configure an S loop:

1. Choose **Services**, **Telephony Services**, **Loops**.

2. Select a loop number (for example, Loop 201).

3. Set the Type to S.

4. Configure the loop settings according to the table:

Attribute	Description
Sampling	Allows you to select a sampling rate for the S-loop. Select Fixed if two or more S-interface devices use the loop and the length of the loop is less than 200 m (650 ft.). Select Adaptive if two or more S-interface devices use the loop and the length of the loop is greater than 200 m (650 ft.). If one S-interface device is using the loop, the length of the loop can be up to 1000 m (3230 ft) and the Sampling rate should be set to Adaptive. Values: **Adaptive**, **Fixed** (Default:
ONN blocking state	Allows you to set the ONN block state. Values: **Suppression bit**, **Service code** (Default: **Suppression bit**)

SPIDs (North America only)

For ISDN BRI service, your service provider supplies service profile identifiers (SPIDs) and Network DNs.

To assign a SPID to a BRI loop:

1. Choose **Services**, **Telephony Services**, **Loops.**

2. Click the key beside the loop number (for example, Loop 201) where you want to assign DNs.

3. Click on the **SPIDs** heading.

4. Choose **Add** above the navigation tree.
   The SPID dialog box appears.

5. Type in the SPID number.

6. Click **Save**.
   SPID 1 appears as a sub-heading.

Assigning the Number of B-channels

To assign the number of B channels to a SPID:

1. From the **SPIDs** heading, click on the **SPID #** you want to configure for this Loop.

2. Select **1** or **2** in the **Number of B-channels** box.

Assigning DNs

To assign Network DNs to the BRI loop:

1. From the **SPID #** heading, click on the **Network DNs** heading.

2. Click the **Add** button above the navigation tree.

3. Type the DN number in the **DN** box.

4. Click the **Save** button.
   DN 01 appears as a sub-heading.

Assigning Call type for a Network DN

Configure the call type for the Network DN, **Voice**, **Data** or **Both**:

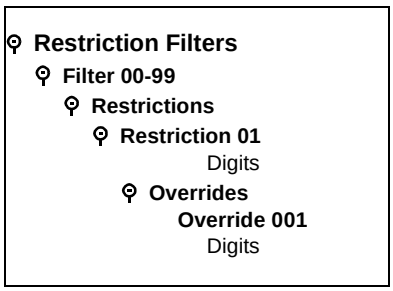
1. From the **Network DNs** heading, click on the **DN ##** that you just assigned.
   The **Loop# /SPID# /DN #** window appears.

2. Select **Voice**, **Data** or **Both** in the **Call type** box.

Restriction filters

Restriction filters prevent you from making certain kinds of calls from a telephone or from lines that are available at the telephone. They also restrict some features.

The following illustration shows the Restriction filters programming map.



Filters

A restriction filter is a set or group of restrictions and overrides that specify the external numbers or feature codes that cannot be dialed from a telephone or on a line. Rather than define individual restrictions and apply them repeatedly to telephones and to lines, the restriction filters setting Allows you to assign them in one step as a single package of dialing sequences that are not permitted.

In addition to restricting telephone numbers, you can prevent people from entering dialing sequences used by the central office (the public network) to deliver special services and features. Because some of these features provide the caller with dial tone after they have entered the special code (which often uses # or *), users may have an opportunity to bypass restrictions. To prevent this from happening, you can create filters that block these special codes.

You create a filter by defining the dialing sequences that are denied. There will also be variations of each sequence that you will want users to be able to dial. Sequences that can be dialed are called overrides.

Once you create the filters, you can assign the restrictions to a telephone (**Terminals & sets**), to a line (**Lines**), to a particular line on a telephone (**Terminals & sets**), and to remote callers (**Lines, Remote access**).

Note: Filter 00 cannot be changed; filters 02—04 have default settings; see Default filters (North America) on page 125.

To program a restriction filter:

1. Choose **Services**, **Telephony Services**, **Restriction filters**.

2. Expand the restriction filter you want to program (Filter 00-99). Click on the **Restrictions** heading.

3. Click **Add** above the navigation tree to enter a restriction for each filter. The Add restrictions dialog box appears.

4. Type the digits that you want to restrict callers from dialing.

5. Click **Save**.

6. Click **Overrides** to view, or click **Add** above the navigation tree to enter overrides for each restriction filter.
   The **Add Overrides** dialog box appears.

7. Type the digits that are an exception to the restriction.

8. Click **Save**.

Note: Enter the letter **A** as a wild card character that represents any digit in a sequence of numbers when denying numbers or creating overrides.

If you delete a restriction, it also deletes the overrides and the restrictions renumber to fill the gap.

Default filters (North America)

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with ten restrictions and some associated overrides. In Filter 01, Restriction 02 and Override 001 allow long distance toll free calls.

The dialing string 911 (the number for emergency assistance in North America) is included as both a restriction and an override in Filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Note: Default filters are only loaded at a cold start.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are the default filters in these programming headings:

Filter	Heading	Sub-heading
02	Terminals & sets	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Tips

Filter 00 cannot be changed. Enterprise Edge can have up to 100 restriction filters (00 to 99).

Each programmable filter can have up to 48 restrictions. There is no limit on the number of overrides that can be allocated to a restriction. There is a maximum total of 400 restrictions and overrides allocated to the 100 programmable filters.

The maximum length of a restriction is 15 digits. The maximum length of an override is 16 digits.

A single letter (A) in a dialing sequence is a wild card (stands for any digit). You can use * and # in a sequence of numbers in either a restriction or an override. These characters are often used as part of feature codes for other systems or for features provided by the central office (the public network).

When restricting the dialing of a central office feature code, do not forget to create separate restrictions for the codes used for DTMF and pulse lines. Examples of dialing strings that may be restricted for this reason are *67 and 1167. Do not string together a central office feature code and a dialing sequence that you want to restrict. Create a separate restriction for each.

You can copy restrictions and overrides from one filter to another. Any restriction or override can be used in any number of filters. Each time it is used, it counts as one entry. For example, if restriction 411 exists in filters 01, 02 and 03, it uses up three entries of the 400 entries available.

Removing a restriction from a filter has no effect on the contents of other filters even if the restriction was copied to them. You cannot delete a filter. Removing the restrictions programmed on a filter makes it an unrestricted filter but the filter itself is not removed.

Exercise caution when removing overrides.

Removing a restriction removes the overrides associated with it. It also changes the identifying numbers of the subsequent restrictions that you may have defined. For example, if you remove Restriction 01, Restrictions 02 to 08 are renumbered as 01 to 07.

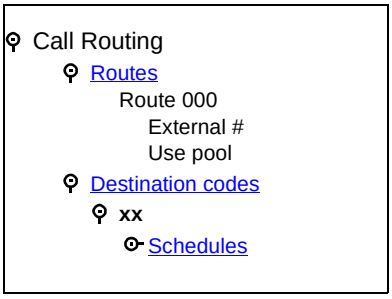
Time & date

1. Click **Time & date**. Enter the time and date in the following format: `yyyyMMddHHmmss`.

You can configure the system to your local time zone under **System**, **Identification**. The system automatically determines and changes the time for Daylight Savings Time if you have ISDN lines.

Call Routing

The Call Routing heading allows you to define how calls are routed by your Enterprise Edge system. The following illustration shows a detailed view of the Call Routing programming map.



Call routing decides what path an outgoing call takes using the digits that are dialed. It is sometimes called Automatic Route Selection (ARS).

When you select an internal line and dial, the system checks the numbers you enter against the routing tables. If the number you dial starts with a destination code, the system uses the line pool and dials out digits specified by the route assigned to that destination code, and then dials the rest of the number that you dialed.

Routing service replaces a number of manual tasks, including:

- entering a line pool code
- dialing an access code for a long distance carrier
- deciding which line pool to use according to the time and day

You can set up routing to take advantage of any leased or discounted routes using information supplied by the customer. The system cannot tell what lines are cheaper to use.

For Call by Call service selection (PRI only), the installer defines destination codes for various call types over PRI lines (for example; Foreign Exchange, Tie Trunk, and OUTWATS). The user simply dials a number using the intercom button without having to enter any special information. For more information see, Call by Call service selection for PRI on page 166.

Using routing to create a coordinated dialing plan is explained in Coordinated dialing plans on page 335.

Plan your routing service before doing any programming.
Routing affects every call placed in the system and must be carefully planned to avoid conflicts and gaps in the programming. Use tables to design routes and destination codes, then check for potential problems before you start programming. It will also save you time to have all the settings written out in front of you.

Routes and destination codes

The settings for a call route include:

- a 3-digit route number (000-999)
- external # digits (up to 24)
- a line pool
- destination codes (max. of 500 available, up to 7 digits)
- DN type
- public DN lengths
- a schedule (programmed in Services)

Tips

To dial a telephone number that does not match any of the programmed destination codes, you must choose a line and dial the number. For long distance dialing, you can program the area codes in the North American numbering plan as destination codes.

Routes

To program a call route:

1. Choose **Services**, **Telephony Services**, **Call Routing**, **Routes**.

2. Click **Add** above the navigation tree. Enter a 3-digit route number (000-999) and click **Save**.

3. Click on the Route number in the navigation tree.
   The Route window appears.

External

External number or dial out number is the number you want the route to use.

4. Enter the digits (up to 24). You can press F78 to insert a 1.5 second pause in the dialing string, or F804 to wait for dial tone, if necessary. Route 000 has no External # by default and cannot be changed.

Use pool

5. Select a line pool for the route: **Pool A**, **Pool B...Pool O** or **PRI-A** to **PRI-F**. The PRI pools only display if you configure an EE-DTM for PRI.

Note: Route 000 uses Pool A by default and cannot be changed.

DN type

The DN type setting shows only for service type Tie.

6. Select **Public** or **Private** DN type.

Call by Call Service routing

The following is an example of a Routing Table containing Call by Call programming (available in the North America market profile).

Route # (000-999)	Dial Out (24 digits)	Use Pool	Service Type	Service Identifier
003		PRI-A	Public	
004		PRI-A	FX	xxxxx
005		PRI-A	Tie	xxxxx
006		PRI-B	OUTWATS	xxx
007		PRI-B	Private	
008		PRI-B	Switched Digital	
Note: The public DN lengths are used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private.				

The service identifier (SID) depends on the selected service type (for example, with NI-2 protocol).

Service Type	Service Identifier description
Public	None
FX	Facility Number 1-5 digits
Tie	Facility Number 1-5 digits
OUTWATS [a]	Optional Band Number 1-3 digits
Private	None
Switched Digital	None
a. For NI-2, do not program the Carrier Access Code for banded OUTWAT calls. This call may be rejected.	

When you select or change a PRI protocol, the Service Type and Service ID fields automatically clear for each entry in the routing table for that PRI.

Programming the PRI routing table

The dialing plan must be thoroughly planned out in advance before programming the information into the Enterprise Edge system.

To program the routing table:

1. Choose **Services**, **Telephony Services**, **Call Routing**, **Routes**.

1. Under **Route001, External #:**, type a number (up to 24 digits).

2. Under **Use pool:**, select a line pool.
   The PRI pool(s) displayed depend on how the PRI lines are put into pools in the Trunk/Line Data section of programming. It is possible to have only pool PRI-A, or only pool PRI-B, or only PRI-C, etc., even if there are three EE-DTMs configured as PRI in the system.

3. Under **ServiceType:Public**, select a different Service Type if required.

4. Under **Service ID:None**, type the Service ID number. This is shown only if the service requires an ID.

5. Under **DN type:Public**, type **Public** or **Private**. This box shows only for service type Tie.

Destination codes

The numbers used for destination codes must not conflict with:

- Call Park Prefix
- External Access Code
- Direct Dial Numbers
- Line Pool Code
- Internal set numbers (intercom)
- DISA DN
- Auto DN

For example, the system will confuse an internal number of 221 and a destination code of 22 because even if the caller dialed the complete internal number, the call would be routed using the first two digits. But an internal number of 221 and a destination code of 23 would work.

In order to make digits available for use with destination codes, you can change the DN length of B1 and B2 DNs depending on your system size. You can change the DN length either at system startup or in **General settings**.

Wild card character

When programming destination codes, you can use wild cards in the destination code string. Wild card characters reduces the number of destination codes programmed in the system.

1. Choose **Services**, **Telephony Services**, **Call Routing**, **Destination codes**.

2. Click on the destination code you want to modify or click **Add** above the navigation tree to enter a new destination code.
   The Destination code dialog box appears.

When you enter a destination code, type the letter A as a wild card character in the destination code.

The wild card character can be used only for the last digit of a destination code and represents any digit from 0 to 9 except for digits already programmed or used by other numbering plans. Should there be a conflict with other digits already programmed or used by other destination codes, an error message appears.

The wild card character can only be used to group destination codes that use the same Route and Digit Absorbed Length.

Route	External #	Line Pool
555	763-4018	Line Pool C
565	763-3492	Line Pool A

Destination codes	Route	Digit Absorb	Dial Out
9201[a]	555	3	763-4018 *-1*
9202	565	3	763-3492 *-2*
9203	555	3	763-4018 *-3*
9204	555	All	763-4018
9205	565	2	763-3492 *-05*
9206	555	3	763-4018 *-6*
9207	555	3	763-4018 *-7*
9208	555	3	763-4018 *-8*
9209	555	3	763-4018 *-9*

a. In this example, the default Line Pool A access code 9 is deleted to make it available for use as a Destination code

Note: The numbers in italics in the Dial Out sequence are not visible to the user.

Destination codes	Route	Digit Absorb	Dial Out
920A	555	3	763-4018 - A
9204	555	All	763-4018
9205	565	2	763-3492 - *05*

Note: The numbers in italics in the Dial Out sequence are not visible to the user.

Normal route

1. Choose **Services**, **Telephony Services**, **Call Routing**, **Destination codes**.

2. Choose the Route you want to configure, and click **Schedules**.

Use route

3. In the Use route setting, select what route a call using the destination code takes during normal service and for each of the schedules. You can program the automatic schedule times under **Scheduled Services**. The default Normal route is 000, it has no External # digits, and uses Pool A.

Absorbed length

4. Select the portion of the destination code that is always absorbed by the system and not used in the dialing sequence. Select the number of digits to be deleted: **0**, **1**, **2**, **3**, **4**, **5**, 6, or **All**.

Tips

The digit absorption setting (**absorbed length**) only applies to a maximum of two schedules. Setting digit absorption to 0 minimizes the effort involved in preparing destination codes. With a 0 setting, the actual digits dialed by a caller are preserved in the dial out sequence. Programming a dial out sequence as part of the route may or may not be necessary depending on the required dialout.

Setting up a route for local calling

An office can have different suppliers for local and long distance telephone service. By programming a destination code, any call that begins with 9 (the most common dial out digit) will automatically use lines dedicated to local service.

The first step is to build a route (under**Call Routing** in **Telephony Services**).

- Type 001 (or any other available route number).

You can view defined routes or erase a defined route.

- Assuming that the lines for local calling have been placed in Line pool A, choose it as the line pool.
- Type the dial out digits (if any) that are needed to direct the call once it is connected to an external line.

The second step of programming is setting up how the route will work with a destination code. Because users will dial 9 to make an external call, 9 should be the destination code.

For local calls only, there are no dial out numbers (compare with Setting up a route for long distance calling on page 134).

- Type 9 at **Destination Code:**.

If entering a code other than 9, a valid destination code must be used. See Destination codes on page 131.

View existing destination codes before entering a new code.

The destination code can use a different route depending on a Schedule (see Services). In the current example, Route 001 is used when someone dials 9 during normal mode (the mode used when the other Schedules are turned off).

- The route for the first schedule appears after **Normal:**. Type the defined route number 001.

The following illustrations show sample tables used for planning and recording routing service. They are filled out to match the examples of routes for local and long distance calling.

Routing Service (Services: Routing Service)

Route # (000-999)	**Dial out** (if required) (max. 24 digits or characters)	**Use Pool**
001	*none*	(A) B C D E F G H I J K L M N O
002	*none*	A (B) C D E F G H I J K L M N O
		A B C D E F G H I J K L M N O
		A B C D E F G H I J K L M N O
		A B C D E F G H I J K L M N O

Destination codes (Services; Routing service; Destination codes)

Service Schedule name (max. 7 char)	**Normal Rte**		**Night Rte**		**Evening Rte**		**Lunch Rte**	
DestCode (max. 7 digits)	**Use route** (000-999)	**Absorb Length**	**Use route** (000-999)	**Absorb Length**	**Use route** (000-999)	**Absorb Length**	**Use route** (000-999)	**Absorb Length**
9	~~000~~ *001*	All		All		All		All
1	~~000~~*002*	~~All~~ *0*		All		All		All
	000	All		All		All		All
	000	All		All		All		All

Setting up a route for long distance calling

An office may have leased lines or T1 E&M trunks which make it cheaper to call long distance. The routing should take place automatically when the number of the outgoing call begins with 1.

Again, the first step is to define a route (under **Call Routing** in **Telephony Services**).

- Type 002 (or any other available route number) at **Route:**
- Assuming that the discounted lines for calling long distance have been placed in Line pool B, choose it as the line pool.
- Type 1 at **Destination Code:**

A valid destination code must be used. See Destination codes on page 131. View existing destination codes before entering a new code.

The destination code can use a different route depending on the Schedule. In this example, the system uses Route 002 (which uses Line pool B) to take advantage of the lower cost when the system is in normal mode.

- The route for the first schedule appears: **Normal:**. Type the defined route number 002.

Tips

The digit absorption setting (**Absorbed Length**) only applies to a maximum of two schedules.

Setting **Absorbed Length** to 0 minimizes the effort involved in preparing destination codes. With a 0 setting, the actual digits dialed by a caller are preserved in the dialout sequence. Programming a dial out sequence as part of the route is not necessary.

If rates change depending on the time of the day or week, a different route can be used for the same destination code 1 when a particular schedule is in use. See Programming for least cost routing on page 136.

Adding a long distance carrier access code

In many cases, long distance service uses the same lines as local service but is switched to a specific carrier using an access number (sometimes called an equal access code). Programming for routing can include the access number so users do not have to dial it every time they make a long distance call.

1. Create a route that uses a line pool containing local lines only.

2. Program the route to use a line pool containing the lines used to access the long distance carriers.

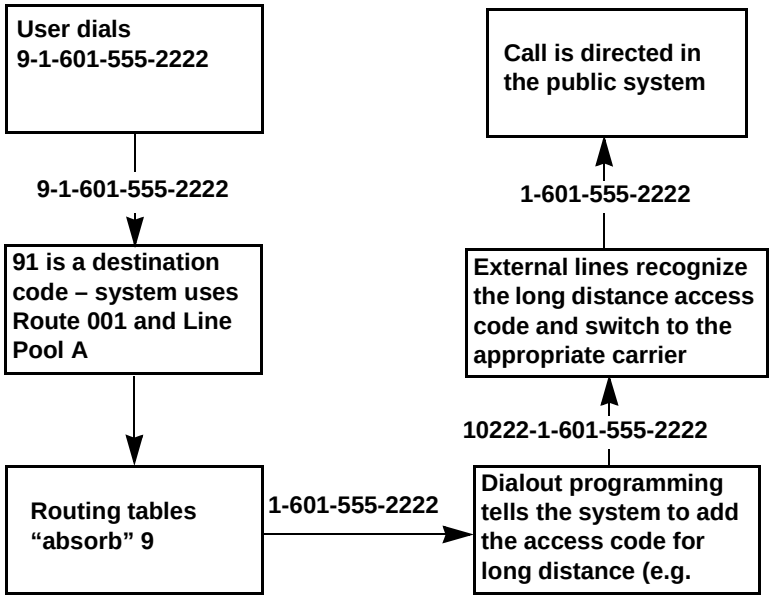
3. Type the dial out digits, which are the same as the access digits. For example, if the access code is 10222, the dial out digit is 10222.

4. Create a destination code 91: 9 (for outside access) and 1 (for long distance). A valid destination code must be used. See Destination codes on page 131.

5. Set **Absorbed Length** to 1. The 9 is only used internally and should be dropped; the 1 is needed to direct the call to the public carrier network.

Tips

The destination codes 9 and 91 used in the examples cannot be used together. If the destination code 91 is needed to direct long distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. See Wild card character on page 131 for information on programming destination codes.


User dials
9-1-601-555-2222
9-1-601-555-2222
91 is a destination code – system uses Route 001 and Line Pool A
Routing tables "absorb" 9
1-601-555-2222
Dialout programming tells the system to add the access code for long distance (e.g.
10222-1-601-555-2222
External lines recognize the long distance access code and switch to the appropriate carrier
1-601-555-2222
Call is directed in the public system

Programming for least cost routing

It may be cheaper to use another long distance carrier at another time of day. Continuing with the example used in the previous flowchart, the lines that supply local service in normal mode will also be used for long distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, another route has to be built.

1. Choose Route 007 (or any other available route) at **Route:**.
2. Choose **No number** for the dial out.
3. Choose **Line pool A** (local service carrier lines).

In this case, the change in route uses the start and stop times for Night Schedule (the schedule for different modes are set up under **Services**).

1. Add 91 as a **Destination code.**
2. The route programmed with the access code as its dial out (Route 001) remains as the route used by **Normal:**.
3. Make sure **Absorbed length** is set at 1.
4. Under **Night route:** select **Route 007**.

Calls that begin with the digits 91 will now travel out without using the access code when the Night schedule comes into use automatically or when you turn it on at a control set.

Using dialing restrictions with routing

Routing service can be further customized by adding dialing filters to lines in line pools. Filters restrict the use of the line to specific area codes.

Tips

Host system signaling codes can be part of the dial out.

You can also use routing as an alternate method for a direct-dial number. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1.

Because overflow routing directs calls using alternate line pools, a call may be affected by different line filters when it is handled by overflow routing.

Using a dialing plan to route outgoing PRI calls

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing outgoing calls. All PRI calls must go through a dialing plan.

The Dialing Plan:

- Allows Enbloc dialing by buffering user-dialed digits until a complete DN has been dialed (Enbloc dialing is a requirement for PRI).
- Provides the ability to map user-dialed digits to a service type on a Call-by-call basis.
- Allows long distance carrier selection via user-dialed Carrier Access Codes.
- Allows incoming calls to be routed according to the service type and the digits received.

Enbloc dialing

The Private DN Length must be set to the number of digits users dial to reach other nodes in the private network. PRI trunks use the Private DN Length parameter to determine when a complete number is dialed. PRI trunks use the PSTN DN Length Table to determine when a complete PSTN DN is dialed. Entries in the table consist of two fields, Prefix and DN Length.

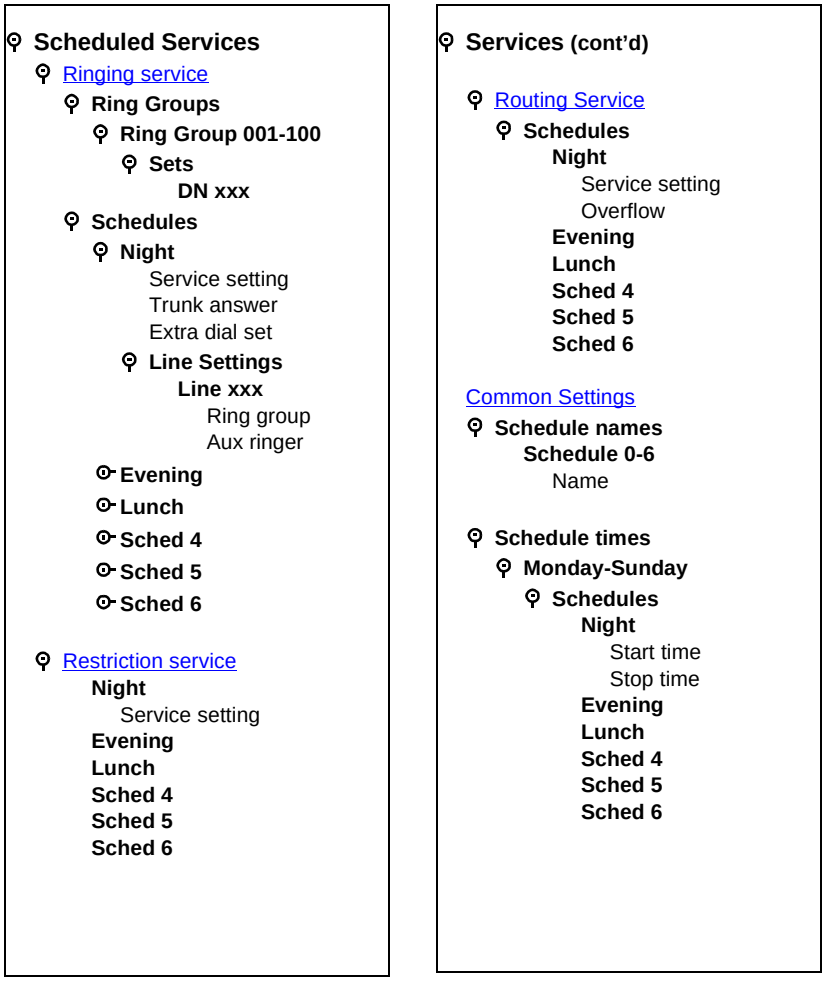
Scheduled Services

The Scheduled Services heading allows you to control three types of service by the time of day and day of week:

- Ringing service for alternate call ringing at certain times and days.
- Restriction service for alternate dialing restrictions at certain times and days.
- Routing service for alternate call routing at certain times and days.

You can also specify common names and times for schedules under the Scheduled Services heading.

The following illustration shows the Services programming map:



Each of the three services has six schedules that you can customize. For example, you may want to combine alternate call ringing with alternate dialing restrictions for lunchtime, evenings, and weekends (Schedules 1, 2, and 3). Then you may want to run alternate call routing using three separate schedules.

Tips

Once you have programmed the different services and schedules, you can turn each of the services on separately. For example, the Night schedule might control both Ringing service and Restriction service. But you can turn on just the Ringing service part of the Night schedule if you wish.

You can activate the services from the designated control telephone for each Enterprise Edge telephone and line in your system. You can have one control telephone for the whole system, or different control telephones for different Enterprise Edge telephones and lines.

If you want to have several services active at the same time, simply program them on for the same schedule.

Ringing service

At certain times or in certain situations, you may want additional telephones to ring for incoming lines. The most common use of this feature is when a security desk telephone rings for incoming lines after 5:00 p.m., a practice often called “night service”.

1. Choose **Services**, **Telephony Services**, **Scheduled Services**, **Ringing service**.

Ring groups

Ring groups allows you to define groups of extended ringing sets. A group can be assigned to any line for any of the schedules. You can define up to 100 ring groups with up to 30 sets for each ring group.

To define a ring group:

2. Choose **Ring groups**.

3. Choose the ring group you want to program (**Ring group 001-100**). The subheading **Sets** appears in the navigation tree.

4. Click on **Sets** and click on **Add** above the navigation tree.

5. In the Add Sets window, type the DN of the set you want to assign to this ring group.

Tips

You can assign any set on the Enterprise Edge system to a ring group. The assigned control set for each schedule is added to each ring group.

A set can belong to more than one ring group.

Schedules

Indicate how Ringing service should be activated for each of the schedules:

1. Choose **Services**, **Telephony Services**, **Scheduled Services**, **Ringing service**.

2. Choose **Schedules**. The navigation tree expands to show all the schedule names.

3. Click on a schedule name (for example, **Night**). The schedule window appears.

Service setting

4. Select whether the Service schedule is **Off**, **Manual**, or **Auto**.

Manual allows you to turn the service on and off at any time from a control set using the Ringing service feature code.

Auto allows you to program a stop and start time for a service. You are still able to start and stop the service by entering the appropriate Services feature code at a control set. If you select this setting, you will have to set start and stop times. See the section on schedule times for information on programming times.

Off prevents the service from being activated.

Trunk answer

Trunk answer allows you to answer, from any telephone, an external call that is ringing at another telephone in your office. This is useful if the other telephones are not assigned the same lines as the telephone you are using to answer the call.

5. Click **Y** or **N** to enable Trunk answer.

Tip
You can change the Trunk Answer setting only if Ringing service is set to Manual or Automatic.

Extra dial set

The Extra dial set attribute allows you to assign an additional direct-dial set for each schedule.

6. Enter the DN of the extra-dial set or choose **None**.

Tip
The extra dial set is activated during a schedule by entering the Ringing service feature code from a direct-dial set. This does not activate the Ringing service unless the direct-dial set is also a control set.

Line settings

For Ringing service, **Ring group** and **Auxiliary ringer use** are programmed for each line individually.

Ring group

You can assign a predefined ring group to a line for each schedule. See Ring group on page 141 to create groups of extra ringing telephones.

7. Choose **Schedules**, **Line settings**.

8. Click on the line number (for example, **Line 061**).
   The schedule/line number window appears.

9. Type in a ring group number (001-100) to choose a different ring group assignment.

Tip

Only one ring group can be assigned to a line for each schedule. To combine groups of ringing sets, you must create a new ring group which contains all the sets you want to ring and assign it to the line.

Aux ringer

Indicate whether the auxiliary ringer (if installed) also rings when Ringing service is on.

10. Click **Y** or **N** to enable Auxiliary ringer.

Tips

The default ringing telephone is 221. This means that all lines ring at telephone 221 when Ringing service is on.

You can copy Ringing set and Auxiliary ringer programming from one line to another.

If you have an auxiliary ringer programmed to ring for calls on an external line, and you transfer a call on that line without announcing the transfer, the auxiliary ringer will ring for the call transfer.

Restriction service

Indicate how the alternate dialing restrictions are activated for each of the schedules:

1. Choose **Services**, **Telephony Services**, **Scheduled Services**, **Restriction service**.

2. Select the schedule you want to program, (for example, **Night**).
   The schedule window appears.

Service setting

3. Select the service setting for the schedule: **Off**, **Automatic**, or **Manual**.

See Service setting on page 140 for descriptions of the three settings.

Routing Service

Indicate how call routing activates for each of the schedules:

1. Choose **Services**, **Telephony Services**, **Scheduled Services**, **Routing service**.

2. Select the schedule you want to program, for example, **Night**. The schedule window appears.

Service setting

3. Select the service setting for each schedule **Off**, **Automatic**, or **Manual**.

See Service setting on page 140 for descriptions of the three settings.

Overflow routing

If all the lines used by a route are busy when a call is made, you can program Routing service to overflow to the route used for normal mode. If this happens, the set sounds a warning tone and displays the message **Expensive route**. The caller can then release the call to avoid using the normal route, or continue with the call.

4. Choose **Y** or **N** to enable or disable Overflow routing. The default is **N**.

Tips

A schedule must be active for overflow routing to be in effect. Overflow routing is not available in normal mode.

You must create an overflow route to be used with each destination code. In this way, every route used with a scheduled mode that has overflow service must have an alternate route in normal service.

Common Settings

Services share the settings for schedule names and schedule times.

1. Choose **Services**, **Telephony Services**, **Scheduled Services**, **Common settings**.

Schedule names

The schedule name shows on the display of the control set when the schedule is turned on. It identifies the active schedule.

2. Click on **Schedule names**. The Schedule name window appears.

3. Type a name of one to seven characters in the **Name** box.

Tips

The default names of the six possible schedules are only suggestions and may be changed to any other name. A schedule name can be one to seven characters long. It is recommended that you reserve certain schedules (4, 5, and 6) exclusively for alternate call routing (Routing service).

Schedule times

Schedule start and stop times are set at times you are most likely to want each service to be active.

4. Click on **Schedule times**.

5. Click on the day you want to program (for example, **Monday**).

6. Click on **Schedules**. The programming menu expands to display all the schedules.

7. Click on the schedule you want program. The Day-Schedule window appears.

8. Type the start and stop times for each schedule, on each day.

Schedule	Start time	Stop time
Schedule 1: Night	23:00	07:00
Schedule 2: Evening	17:00	23:00
Schedule 3: Lunch	12:00	13:00
Schedule 4: Schedule 4	00:00	00:00
Schedule 5: Schedule 5	00:00	00:00
Schedule 6: Schedule 6	00:00	00:00

Tips

It is only necessary to program start and stop times for schedules that are activated automatically. See the instructions with Ringing service for information on activating schedules.

The time may be entered in either 12 or 24-hour format. If the display is in English, and the hour entered is less than thirteen, the display prompts you to specify **AM** or **PM**.

If you assign identical start and stop times for a schedule, for example, 04:00 start and 04:00 stop, the schedule is in effect all day. The only exception to this is a start and stop time of 00:00; in this case the schedule is off for the day.

You may assign overlapping times. For example, if schedule 1 is assigned from 9:00 am to 4:00 pm and schedule 2 is assigned from 1:00 pm to 5:00 pm, then the start time of the second schedule is treated as a stop time for the first schedule.

This is also true if two schedules have the same start time but different stop times; the stop time of the shorter schedule is treated as the start time of the longer schedule.

If one schedule starts and stops within the times of another schedule, the first service temporarily ends when the second service starts. The first service then resumes when the second service has ended.

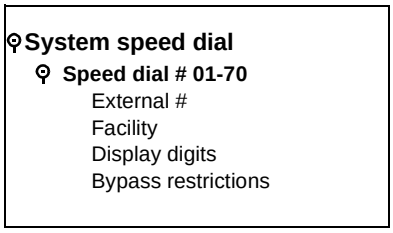
Some schedules start and stop at the same times each day: use **COPY** to copy the start and stop times from one day to the next.

Start and stop times do not span days.

When you program a schedule to start in the evening and stop in the morning, it does not carry over into the next day. For example, if you program Night service for Friday (22:00 to 6:00), the system turns on Night service from midnight to 6 am on Friday, and then again from 10 pm to midnight on Friday.

System speed dial

The System speed dial heading allows you to specify speed dial codes (01 - 70) and external numbers that any telephone set on the system can use. The following illustration shows the System speed dial programming map.



Adding or changing a system speed dial

You can program a speed dial on your Enterprise Edge system so that anyone in your office can dial a frequently-used number using a two-digit code. Examples of system speed dials might include telephone numbers of regional sales offices within your organization or key customers that you call frequently.

To change a speed dial that already exists, follow the same steps as if you are creating a new system speed dial. The new programming overwrites the previous number and settings.

If you are creating a system speed dial for the first time you will need to choose the type of facility for the system speed dial. For more information about programming line facilities, see Line type on page 116.

The system has a standard name to display, so it is not necessary for you to program one; however, if you choose not to display the telephone number, you may want to create a more descriptive name.

To create a system speed dial:

1. Choose **Services**, **Telephony Services**, **System speed dial**.

2. Click a speed dial (Speed dial # 01 to 70).

3. In the **External #** box, type the telephone number (up to 24 digits), and then press **Enter**.

   If this is a new speed dial, more fields appear after you press Enter.

4. Click a Facility value: **Use prime line**, **Use line:nnn**, **Pool code:x**, or **Use routing table**.

   Note: If you assign a specific line to a system speed dial number, only telephones with an appearance of that line can use the speed dial number.

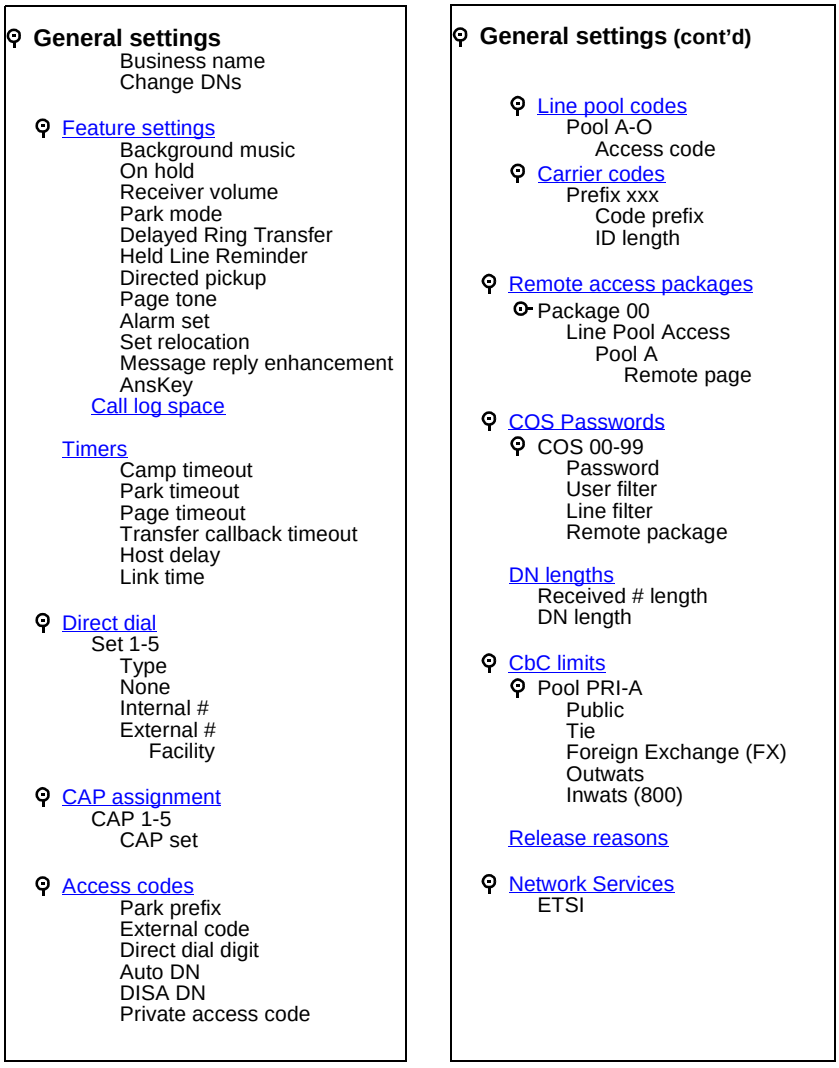
5. Click a Display digits value: **Y** (Yes) or **N** (No).

   Note: If you choose not to display the digits, the name of the Speed Dial code is displayed instead of the phone number. The default is Y.

6. Click a Bypass restrictions value: **Y** (Yes) or **N** (No). The default is **N**, the Speed dial number will not bypass the line and set restrictions already programmed.

General Settings

The General Settings heading allows you to define system-wide settings. The following shows the General Settings programming map.



Business name

The Business name setting allows you to type in a name that will show on the display of the person you are calling.

To change the Business name:

1. Choose **Services**, **Telephony Services**, and then click on the **General settings** heading.
   The General settings screen appears.

2. Type a name up to 7 characters and then press **Enter**.

Change DNs

Change DNs allows you to change the directory number (DN) or internal number of a telephone in the Change DNs dialog box.

Changing DN locks programming session.
Changing an individual DN locks the programming session into the Change DNs programming mode. To unlock the programming session, exit and restart Unified Manager.

1. Choose **Services**, **Telephony Services**, and then click on the **General settings** heading.
2. On the **Configuration** menu, click **Change DNs**.
   The Change DNs dialog box appears.
3. In the **Old DN** box type the DN you want to change.
4. In the **New DN** box type the new DN.
5. Click **OK**.

Note: To change the start DN for your system see System startup on page 259 of the Maintenance chapter.

Feature settings

The Feature settings attribute allows you to program a number of features that apply to all telephones connected to Enterprise Edge.

To configure Feature settings:

1. Choose **Services**, **Telephony Services**, **General settings**, **Feature settings**.
2. Configure Feature settings according to the table:

Attribute	Description
Background music	Allows you to listen to music through your telephone speaker. A music source must be connected to Enterprise Edge. Values: **Y** or **N** (Default: **N**)
On hold	Allows you to choose what a caller hears on an external line when the line is put on hold. Tones provides a periodic tone. Music provides any signal from a source such as a radio connected to Enterprise Edge. Silence provides no audio feedback. Values: **Tones**, **Music**, **Silence** (Default: **Tones**)

Attribute	Description
Receiver volume	Allows you to specify if the volume level of a receiver or headset returns to the system default level when a call ends or is put on hold, or if it remains at the volume level set at the individual telephone. Values: **Use sys volume**, **Use set volume** (Default: **Use sys volume**)
Park mode	Allows you to define how retrieval codes are assigned to parked calls. For more information, see Park mode on page 150. Values: **Lowest** or **Cycle** (Default: **Lowest**)
Delayed Ring Transfer	Defines whether unanswered external calls are automatically forwarded to a prime telephone after a certain period of time. You can estimate the delay in seconds if you multiply the number of rings by six. **Note:** You must assign a prime telephone for this feature to operate. Assign a prime telephone to one or more external lines in Line Data programming. Values: **1**,**2**,**3**,**4**,**6** or **10** (Default: **4**)
Held line reminder	Reminds you that a call at your telephone is still on hold. You periodically hear two tones from your telephone until you return to the call on hold. Choose the number of seconds before the Held line reminder feature begins at a telephone that has an external call on hold. Values: **Off**, After **30**, **60**, **90**, **120**, **150** or **180 Seconds** (Default: **After 60 Seconds**)
Directed pickup	Allows you to answer any calls by specifying the ringing telephone's internal number. Directed pickup is useful when not all the telephones have the same lines, but you want to allow co-workers to answer a call on any external line from their telephones. **Note:** Do not confuse Directed pickup with the Group pickup feature. Group pickup, allows you to answer a call at any telephone within a specific group without specifying the internal number of the ringing telephone. Values: **Y** or **N** (Default: **Y**)
Page tone	Defines whether a tone sounds before a page begins. Values: **Y** or **N** (Default: **Y**)
Alarm set	Allows you to assign a telephone on which alarm messages appear when a problem has been detected in the system. Alarms are recorded in the Windows NT event log. Values: **None**, **DN:** (Default: **221**)

Attribute	Description
Set relocation	Allows you to move any telephone to a ne wlocation without losing the directory number, autodial settings, personal speed dial codes, and any programming for that telephone. **Note:** Activate Set relocation after you do the set installation and programming, for more flexibility in testing equipment. If you deactivate Set relocation while moving a set, the internal number and programming data remain with the physical port on Enterprise Edge. When you connect the set somewhere else, it does not receive the original programming. Values: **Y** or **N** (Default: **N**)
Message reply enhancement	Activates the Message Reply Enhancement feature. For more information, see Message reply enhancement on page 150. Values: **Y** or **N** (Default: **Y**)
Answer key	Allows you to determine what types of calls will alert at the telephone. For more information, see Answer key on page 151. Values: **Basic**, **Enhanced**, or **Extended** (Default: **Basic**)

Park mode

The Call park feature allows you to suspend a call and lets someone retrieve the call by entering a retrieval code at any Enterprise Edge set in the system. Park mode is the setting that determines how the system assigns a retrieval code to parked calls.

Select the way that the system will choose a Call park code: **Lowest** or **Cycle**.

When set to **Lowest**, the system chooses the lowest code that is available when the call is parked. When set to **Cycle**, the system will choose the codes in a sequence, from lowest to highest, until all the codes have been used.

Message reply enhancement

The Message reply enhancement feature allows you to automatically deactivate the message waiting indicator on analog telephones connected to an Enterprise Edge Analog Station Media Bay Module (EE-ASM), if the reply call from the analog telephone to the direct-dial telephone is answered, no matter where the call is answered from by the user.

This feature also functions if the user invokes the Call pickup feature to answer the reply call from the analog set. It does not however, work with the Retrieve parked call feature.

Tips

Direct dial sets are the only sets that can send messages (using Feature 1) to analog telephones connected to an Enterprise Edge Analog Station Media Bay Module (EE-ASM). The direct dial set must be the designated direct-dial set for the analog telephone receiving a message.

Answer key

There are up to eight answer keys that you can assign to a set. The Answer key setting in Feature settings programming Allows you to determine what types of calls alert at the telephone. Answer key changes do not apply to portables.

Your choices are: **Basic**, **Enhanced** and **Extended**.

With the default Basic setting, answer keys do not ring for:

- Prime set call capture
- Call forwarded calls
- Other answer key calls
- Priority calls
- Voice calls
- Ringing service
- Callbacks

The Enhanced setting is the same as the Basic setting except that answer keys will ring for overflow call routed calls (special case of Prime set call capture). Answer keys will not ring for line transferred calls (although Basic will ring).

Extended will ring for all call types except priority calls and voice calls.

Select the setting: **Basic**, **Enhanced**, and **Extended**.

A Phantom DN is a line that can be programmed to appear and ring on a set that does not physically exist. It allows you to create an Answer key for the set that does not exist.

Call log space

The Call log space setting allows you to reallocate the Call log space equally to all telephones in your system.

To Reset log space:

1. Choose **Services**, **Telephony Services**, **General settings**, **Feature settings, Call log space**.

2. On the Configuration menu, click **Reset logs**. The Property sheet window appears.

3. Type the space allocation for the Call log at each telephone. In the **Space per log** box of the Property sheet window, type a three-digit number (for example, 020, to give each set 20 spaces).

4. In the **# of sets with logs** box in the Property sheet window, type the number of sets with logs.

5. Click **OK**. The system automatically reallocates log space.

Tips

Use this heading only if you want to allocate an equal amount of log space to all the telephones in your system.

Reallocating Call log space may destroy Call log data at telephones that lose space.

There are 600 Call log spaces available in the system. There are no spaces allocated by default. Changing the space allocation using Log defaults defines the log space available to all telephones in the system.

Timers

The Timers setting allows you to define a number of timer settings for your Enterprise Edge system. These settings apply to all telephones connected to the Enterprise Edge system.

To configure Timers:

1. Choose **Services**, **Telephony Services**, **General Settings**, **Timers**.

2. Configure settings according to the table:

Attribute	Description
Camp timeout	Allows you to assign the number of seconds before an unanswered camped call returns to the telephone that camped the call. Values: **30**, **45**, **60**, **90**,**120**, **150** or **180** seconds (Default: **45**)
Park timeout	Allows you to assign the number of seconds before a parked call on an external line returns to the originating telephone. Values: **30**, **45**, **60**, **90**, **120**, **150**, **180**, **300** or **600** seconds (Default: **60**)
Page timeout	Defines the period of time after which the paging feature automatically disconnects. Values: **15**, **30**, **60**, **120**, **180**, **300**, **600 2700** seconds (Default: **2700**)
Transfer callback timeout	Allows you to specify the number of rings before a callback occurs on a transferred call. You can estimate the delay in seconds if you multiply the number of rings by six. Values: **3**, **4**, **5**, **6** or **12** (Default: **3**)
Host delay	Assigns the delay between the moment an outgoing line is selected to make an external call (for example, by lifting the receiver off the telephone) and the moment that Enterprise Edge sends dialed digits or codes on the line.This ensures that a dial tone is present before the dialing sequence is sent. Minimizing this delay provides faster access to the requested features. Values: **200**, **400**, **600**, **800**, **1000**, **1200**, **1400**, **1600**, **1800** or **2000** milliseconds (Default: **1000**)

Link time	Allows you to specify the duration of a signal required to access a feature through a remote system. The Link time depends on the requirements of the host switching system. For example, to program external dialing through a Centrex system requires a Link time of 400 ms. Link is another name for recall or flash. Values: **100**, **200**, **300**, **400**, **500**, **600**, **700**, **800**, **900** or **1000** milliseconds (Default: **600**)

Direct dial

The Direct dial setting allows you to dial a single system-wide digit to call a specific telephone, called a direct dial telephone. The most common example of a direct dial set is a telephone for an operator, a receptionist or an attendant. A total of five direct dial sets can be programmed on the system.

To configure Direct dial sets:

1. Choose **Services**, **Telephony Services**, **General Settings**, **Direct dial**.

2. Click on the Direct dial set you want to program (**Set 1**-**Set 5**). The Set # window appears.

Type

3. Choose if the Direct dial set has an **Internal** or **External** number or **None**.

Internal/External#

4. Type the internal or external number that the system automatically dials when someone enters the direct dial digit. The default number for the Direct dial set is **DN 221**.

Facility

If you assign an external number as a direct dial set, you must indicate what line to use for the call.

5. Select the facility (line) for the external number: **Use line:**, **Pool A** to **O**, **Use prime line**, **Use routing table**.

Tip

There is just one direct dial digit for the entire system. Enterprise Edge cannot verify that the number you assign as an external direct dial set is valid. Check the number before assigning it as a direct dial set, and call the direct dial set after you've assigned it in order to test it.

CAP assignment

The CAP assignment setting designates a telephone as a central answering position (CAP). The CAP must be an M7324 telephone, and may have one or two CAP modules attached. You can install a maximum of five CAPs on Enterprise Edge.

The CAP can:

- Monitor the busy/not busy and Do not disturb status of Enterprise Edge telephones.
- Answer external calls on up to 120 lines, and extend calls to other Enterprise Edge telephones.
- Send up to 30 messages to other Enterprise Edge telephones.
- Provide up to 96 extra memory buttons for the M7324 telephone.

To configure a CAP assignment:

1. Choose **Services**, **Telephony Services**, **General Settings**, **CAP assignment**.
2. Click on the CAP you want to program (**CAP 1**-**CAP 5**). The CAP # window appears.
3. Type the set number of the M7324 telephone you want to designate as a CAP.

Tips

If CAP modules are attached to an M7324 telephone that has not been programmed as a CAP, then no CAP settings are assigned. If a CAP module (or modules) is relocated with the M7324 telephone, the settings are retained.

Dialing plan

Dialing timeout

Dialing timeout specifies how long Enterprise Edge will wait between user-dialed digits. This value allows Enterprise Edge to determine when the user has stopped dialing.

The user can also use the '#' key to tell Enterprise Edge that they are finished dialing however, this is not usually required except for international calls where the number of digits dialed varies.

1. Click on **Dialing plan**. The Dialing plan window appears.
2. In the **Dialing timeout** box select a timeout value. You can select the following values (in seconds): **3, 4, 5, 6, 8, 10, 15**.

Note: A timeout value that is too small forces you to enter the digits very quickly one after the other. A value that is too large causes the system to wait for a long time after the last digit is entered before the call is actually made.

For more information on non-PRI routing tables and destination codes, see Routing Service on page 142.

Private network

The Private network settings allows you to configure the type of network (CDP, UDP), the location code and private network DN length.

Type

You can specify if your Private network uses a coordinated dialing plan (CDP) or a universal dialing plan (UDP).

1. From **Dialing plan**, click on the **Private network** heading.
2. Choose the type of private network, **CDP** or **UDP**. The default is **None**.

Private DN lengths

The Private DN lengths parameter specifies the length of DNs in the private dialing plan. This is used by all PRI calls where the route uses DN Type: Private.

1. From **Dialing plan**, click on the **Private network** heading.
2. Select a **Private DN length** (**3**-**14**).

Public network

Public DN lengths

- In most cases it is not necessary to change the default values. The public DN lengths table is used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private. The public DN lengths table allows Enterprise Edge to determine the length of a DN based on the initial digits dialed by the user. In the public DN lengths table:
- You can define at most 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 to 25).
- Several entries will be predefined in North America (can be removed or modified). These defaults will handle most regions in North America without the need for additional programming.
- The table always contains one ‘default’ entry; this cannot be removed. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

1. Under **Dialing plan**, **Public network**, **Public DN lengths**, click on a prefix number (0, 00, 01, 011, 1, 411, 911).

2. Under **DN prefix:**, type the DN prefix number (2 digits, 1 to25).

3. Under **DN length:**, type a DN length number (2 digits, 1 to 25).

Access codes

The system uses Access codes to direct calls to the correct lines and destinations. If the codes conflict, some of the features on the system will not work.

The table of default settings can help you plan your access codes so there are no conflicts.

Digit	Use	Heading
0	Direct dial digit	Access codes
1	Park prefix	Access codes
2	The first digit of B1 DNs	Startup
9	Line pool A access code (Takes precedence over the External line access code if there is a conflict.)	Access codes
— —	External line access code	Access codes
— —	Destination code	Services

To program Access codes:

1. Choose **Services**, **Telephony Services**, **General Settings**, **Access codes**.

2. Double click on **Access codes**. The Access codes window appears.

Park prefix

The Park prefix is the first digit of the call park retrieval code that you enter to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked.

3. Select the setting: **None**, or **1**, **6, 7, 8**.

Tips

The Park prefix cannot be the same as: the Direct dial digit, the External line access code, the first digit of a DN, the first digit of a line pool access code, or the first digit of a destination code.

Other programmable settings may affect what numbers appear in the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes. (To avoid a conflict, refer to the table of default settings in the description of External code.)

If DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

External code

The External code setting allows you to assign the external line access code for M7100 telephones and Enterprise Edge ATA 2s to access external lines.

4. Select the setting: **None,** or **6, 7, 8**.

Tips

The external line access code cannot conflict with: the Park prefix, the direct dial digit, the first digit of a line pool access code, the first digit of a DN, or the first digit of a destination code.

If DN range, and the changed DNs conflict with the external line access code, the setting changes to None.

Direct dial digit

The Direct dial digit setting allows you to specify a single system-wide digit to call a direct dial telephone.

5. Select the setting: **None**, or **0, 6, 7, 8**.

Tips

Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming.

The Direct dial digit cannot be the same as the first digit of a DN, of a line pool access code, the external line access code or the Call park prefix. It cannot be the first digit of a destination code.

If DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.

Auto DN

Calls answered without DISA require no password to access Enterprise Edge. The Class of Service (COS) that applies to the call depends on the COS for the trunk.

6. Type in the Auto DN digits to be received from the auto-answer trunk.

Tips

The length of the Auto DN is the same as the Received Number Length specified in **General Settings**.The Auto DN is cleared if the Received Number Length is changed.

The Auto DN cannot be the same as a line pool access code or a destination code.

DISA DN

For calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (COS) that applies to the call is determined by this COS password.

Once a remote user accesses Enterprise Edge, they can change the existing COS using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access and separate COS passwords with different dialing out privileges for individuals.

7. Type the DISA DN digits to be received from the auto-answer trunk.

Tips

The length of the DISA DN is the same as the Received number length specified in **General Settings**. The DISA DN is cleared if the Received number length is changed.

The DISA DN cannot be the same as a line pool access code or a destination code.

Private access code

The Private access code is the first digit the user dials to access private facilities. It provides access to tandem and toll bypass functionality. For example, a PSTN user in Toronto could call a PSTN user in Ottawa and have the call routed over the private network connection from the Toronto office to the Ottawa office and then out to the PSTN from the Ottawa office. This bypasses any long distance toll charges. To add this functionality, the destination code has to include the private access number. For an example of a toll bypass network configuration and its associated programming, see Toll bypass with Enterprise Edge VoIP Gateway on page 351.

8. Type the Private access code (up to two digits).

Line pool codes

The Line pool codes setting allows you to assign a line pool access code for each of the fifteen line pools (A to O). These codes specify the line pool for making an outgoing external call.

1. Choose **Services**, **Telephony Services**, **General Settings**, **Access codes**.

2. Click on **Line pool codes**. The navigation tree appears Pool A-Pool O.

3. Click on the Pool you want to program. The Pool window appears.

4. Type the Access code. The default Access code is **9** for **Line Pool A**, for **Line Pool B** to **O**. No default is specified for Line Pools B to O.

For PRI, see Line Pools on page 169.

Tips

The code can be one to four digits.

A line pool access code can be the same as an external line access code. In this case, the line pool access code takes priority over the external line access code, and a line from the line pool is selected.

A line pool access code cannot conflict with the Park prefix, the Direct dial digit, the first digit of any Received number, the first digit of any DN (including the Auto DN or the DISA DN).

To avoid a conflict, refer to the table of default settings in the description of External code.

Carrier codes

A multi-digit Carrier access code contains an Equal Access Identifier Code followed by a Carrier Identification Code. The CIC identifies the carrier that handles the call. The Carrier Access Code table stores the CAC digit pattern that you define for your region. In most cases it is not necessary to change the default values. The capability is there to modify overall patterns if required.

- You can define at most five entries.
- Two entries will be pre-defined in North America, but you are free to remove these defaults.
- Each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 - 9).
- Each entry is identified by the prefix digits themselves.

1. Select **General settings, Access codes, Carrier codes**.
2. Click on a Prefix number or choose Add above the navigation tree to add a new Prefix.
3. In the **Code prefix** box, type in 1 to 6 digits.
4. In the **ID length** box, type a carrier ID length value (one digit, 1 to 9).

Remote access packages

The Remote access packages setting allows you to control the remote use of Enterprise Edge line pools. Create a remote access package by defining the system line pools remote users can access. You then assign the package to individual lines (see Use remote package on page 110), and to a particular Class of Service password (see COS Passwords on page 160).

To program Remote access packages:

1. Select **Services**, **Telephony Services**, **General settings, Remote access packages**.

2. Click on a Remote access package number (**00** to **15**).
   The Package window appears.

Remote page

The Remote page setting allows you to determine if the Remote access package allows Remote paging.

3. Type in **Y** or **N** to enable remote paging for each pool in the Remote access package.

Line pool access

4. Click on **Line pool access**, and then click **Add** above the navigation tree.

5. Enter a line pool access code, and then click **Save**.

COS Passwords

Class of Service (COS) passwords permits controlled access to a system's resources by both internal and remote users. When you enter a Class of Service password at a telephone, the restriction filters associated with your Class of Service password apply instead of the normal restriction filters. Similarly, when a remote user enters a Class of Service password on an incoming auto-answer line, the restriction filters and remote package associated with their Class of Service password apply instead of the normal restriction filters and remote package.

COS Passwords allows you to define individual passwords and determine the restriction filters and remote package associated with each.

Tips

The Class of Service passwords for a system should be determined randomly and should be changed on a regular basis.

Users should memorize their COS passwords instead of writing them down. Employees' COS passwords should be deleted when they leave the company. Typically, each user has a separate password. Alternately, several users can share a password or one user can have several passwords.

A system can have a maximum of 100 six-digit COS passwords (00 to 99).

You can copy the restriction filters and remote package from one COS password to another. COS passwords must be unique.

To assign a COS password:

1. Choose **Services**, **Telephony Services**, **COS Passwords**.

2. Click a COS group (**COS 00-99**).
   The **COS nn** window appears.

Password

3. Type a 6-digit password in the **Password** box and press **Enter**.

User filter

User filter allows you to assign a restriction filter to a Class of Service password. The user filter associated with the Class of Service password replaces any normally applicable set restriction, line/set restriction, and remote restriction. The default setting (**None**), means that any normally applicable filters (set restriction, line/set restriction, or remote restriction) still apply.

4. Select a User filter value: **None** or **Filter:**. If you select **Filter:**, type the 2-digit user filter and press **Enter**.

Line filter

The **Line filter** box allows you to assign a specific line restriction to a Class of Service password. The line filter associated with the Class of Service password replaces any normally applicable line restriction. The default setting (**None**), means that any normally applicable line filter still applies.

5. Select a Line filter value: **None** or **Filter:**. If **Filter:** is selected, type the 2-digit line filter and press **Enter**.

Remote package

6. Click a Remote package value: **None** or **Package:**. If you select **Package:**, type the 2-digit remote package and press **Enter**. See Remote access packages on page 160 for more information.

DN lengths

The DN lengths setting allows you to change the number of digits for the Received number length and the DN length.

To assign DN lengths:

1. Choose **Services**, **Telephony Services**, **General settings**, **DN lengths**.
   The DN lengths window appears.

Received # length

The Received number length setting allows you to change the number of digits received on auto-answer trunks. These digits identify target lines, Auto DNs, and DISA DNs.

2. In the **Received # length** box, select the setting: **2, 3, 4, 5, 6**, or **7**.

Tips

The target line number (for example, line 241) and the Received number for the target line (for example, **Received number: 123** for line 241) are two different numbers.

The Received number length may be the same as the system DN length, or may, because of network or central office constraints, be set to some other value.

Changing the Received number length causes all programmed received digits to be cleared.

DN length

The DN length setting allows you to change the number of digits for all DNs. The maximum length is seven. The default and minimum length is **3**.

3. In the **DN length** box, select the setting: **3**, **4**, **5**, **6**, or **7**.

4. Press the Tab key to save the new DN length.
   The prompt appears, “If Nortel Networks Voice Message is installed all messages and mailboxes will be deleted.”.

5. Click **OK** to save the new DN length. Click **Cancel** to restore the original value.

Do not change DN length immediately after a system startup.
You must wait for at least two minutes after a system startup before you change the DN length.

Data devices drop calls when you change the DN length. (These data devices use the B2 channel. The M7100, M7310, and M7324 telephones use the B1 channel. Calls are **not** dropped for these telephones.)

The DN length change takes two minutes, depending on the size of the Enterprise Edge system. System response may briefly slow down during this time.

Tips
On a newly installed Enterprise Edge system, change the DN length first before continuing with other programming.

Each increase in length places the digit 2 in front of any existing DN. For example, if DN 234 was increased to a length of 4, the new DN would be 2234.

If the DN length change so creates a conflict with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code changes to None, and the corresponding feature is disabled.

Network Name Display

Enterprise Edge displays the name of the calling party, when available, on both Private or Public ISDN PRI interfaces. The displayed name may include the Receiving Calling Name, Receiving Redirected Name, and/or Receiving Connected Name. The outgoing name is the Business name concatenated with the Set name. The outgoing name is not supported on BRI (North America). For information on programming your CLASS assignment, see Feature assignment on page 106.

Note: Network Name Display is an optional feature that is available based on the interface you subscribe to.

Feature	Interface			
	NI PRI	DMS Custom PRI	SL-1	NI-BRI
Receiving Calling Name	Supported	Supported	Supported	Supported
Receiving Redirected Name	Supported			Supported
Receiving Connected Name		Supported	Supported	
Sending Calling Party Name	Supported	Supported	Supported	
Sending Connected Name		Supported	Supported	

Receiving and Sending Calling Party Name

Network Name Display allows the name of an incoming PRI/BRI call to be displayed on the Enterprise Edge set receiving the call.

Calling Party Name with status of 'PRIVATE' may be displayed on the Called Party set as '**Private name**'. If the incoming Calling Name is defined by the CO as a private name, then '**Private name**' appears on the answering set. If the Calling Party Name is unavailable it may be displayed on the Called Party set as '**Unknown name**'.

The system supports sending the calling party name (Business name and Set name concatenated together) on calls originated by the Enterprise Edge system.

For information on programming your CLASS assignment, see Feature assignment on page 106. The Set Name will only be sent if the OLI for the Set is configured. See OLI number on page 95.

Receiving Redirected Name

Network Name Display allows the receiving of the Originally Called Name (Redirecting Name) on incoming calls. The Originally Called Name will be stored, but not displayed.

Receiving and Sending Connected Name

Network Name Display supports the reception of Connected Name on outgoing calls. The Connected Name is stored and displayed on the Enterprise Edge set.

In order for this to work you need to set the Called ID to yes. See Auto called ID on page 107.

The system also supports sending the Connected Name (Business and Set Name concatenated together) on incoming calls.

If the call is answered by a hunt group, the hunt group name is used instead of the set name in forming the connected name.

The Connected Name is a transient display that appears for about 3 seconds.

Note: The Connected Name will only be sent if the OLI has been programmed. See OLI number on page 95.

Network Name Display interactions

Calling and Connected Name information (if available) is passed between trunks with Selective Line Redirection (SLR). Only Calling Name information is passed between trunks in cases where Direct System Inward Access (DISA) has resulted in tandeming of trunks.

Programming Network Name Display

The Business name and the Set name make up the information that is used for the outgoing Calling name or connected name.

Calling/connected name is only sent once the Business name is programmed. To program the Business name, see General Settings on page 147. It is recommended that you use a blank space for the last character of the Business name to act as a separator between the Business name and Set name.

To program the Set Name:

1. Under **Services**, **Telephony Services**, **Terminals & sets**, **General settings** select the set number of the telephone
2. In the **Business name** box, type the Business name (7 characters).
3. Other areas that must also be programmed include:
   - The OLI number, see OLI number on page 95.
   - Under Telco Features, the Call ID must be set to Yes, see Auto called ID on page 107
   - Under Lines, type the set number where you want the CLID to appear, see CLID set on page 113.

Outgoing name and number blocking (ONN)

When you activate, Feature 8 1 9 blocks the outgoing name and number (ONN) on a per call basis. When you use this feature, the system flags the call to the CO so that the name and number does not present to the person you call.

Enterprise Edge alerts the CO by two methods and each depends on the type of trunk involved in placing the outgoing call. Analog trunks use a dialing digit sequence called a Vertical Service Code (VSC). The VSC differs from region to region and must be programmed. Analog trunks with both tone and pulse dialing trunks can have separate VSCs. PRI trunks have only one VSC.

To configure ONN:

1. Under **Services**, **Telephony Services**, **Telco features**, two options are available.
2. For analog trunks under **Voice message center numbers, ONN blocking, Analog VCS, Tone:None.** You can choose F78, (0-9), *, #.
3. Type a new tone dialing Name and Number blocking digit sequence.
4. For non-analog trunks under **Voice message center numbers, ONN blocking, Pulse:None.** You can choose F78, (0-9), *, #.
5. Type a new pulse dialing Name and Number blocking digit sequence.

Call by Call service selection for PRI

Call by Call service selection allows you to access services or private facilities over a PRI line without the need for dedicated facilities. The different services represent different types of access to the network. Various services (see list below) are available depending on the chosen protocol.

Call by Call service selection is supported for the following protocols:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250 (MCI, Sprint, Generic)
- AT&T 4ESS custom

The following Call by Call Services are supported:

- Public

  Public calls connect Enterprise Edge and a Central Office (CO). Both incoming (DID) and outgoing (DOD) calls are supported. Dialed digits conform to the standard North American dialing plan (E.164 standard).

- Foreign Exchange (FX)

  Foreign exchange service connects an Enterprise Edge site to a remote central office (CO). This provides the equivalent of local service at the remote location.

- Tie

  Tie lines are private incoming and outgoing lines that connect Private Branch Exchanges (PBXs) such as Enterprise Edge.

- Outward Wide Area Telecommunications (OUTWATS)

  This outgoing call service allows an Enterprise Edge user to call telephones in a specific geographical area referred to as a zone or band. Typically a flat monthly fee is charged for this service.

- Inward Wide Area Telecommunications (INWATS)

  This long distance service allows an Enterprise Edge user to receive calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.

- International INWATS

  An international long distance service that allows an Enterprise Edge user to receive international calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.

- Switched Digital

  This service provides premises to premises voice and data transport with call management and monitoring features.

- Nine Hundred

  This service is commonly referred to as fixed charge dialing.

- Private

  Private incoming and outgoing calls connect Enterprise Edge to a virtual private network. Dialed digits may conform to the standard North American dialing plan (E.164 standard) or the dialed digits may use a private dialing plan.

Enterprise Edge Service types[1]	NI-2	DMS-100 (custom)	DMS-250 (MCI, Sprint, Generic)	AT&T 4ESS
FX	FX	FX[2]		
Tie[3]	Tie	Tie	Tie	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International INWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTWATS	OUTWATS	PRISM	MEGACOM
Private		DMS Private[5]	VNET (virtual network)	
Switched Digital				ACCUNET[4]
Nine Hundred			Nine Hundred	MultiQuest
Public	Public	Public	Public	

1. A shaded box indicates that the protocol does not support the service.
2. DMS-250 Sprint and UCS support incoming FX only (i.e. Network-to-Enterprise Edge). DMS-250 MCI does not support FX.
3. NI-2 allows two Tie operating modes: senderized and cut-through. Enterprise Edge will only support senderized mode.
4. Rates greater than 64 kbps will not be supported.
5. Bell Canada VNET.
6. Not all service types may be supported by a switch type. For information, contact your service provider.

Programming Call by Call on PRI requires you to program various areas of the Enterprise Edge system such as:

- Under **Line Access**, assign the line pool.
- Under **Services**, in routing services section, assign which pool to use for routing and which service type, and service id if required.
- Under **General settings**, specify the minimum and maximum values for the pools.

- Under **Hardware**, choose DTI (PRI) and select the protocol

Programming Call by Call service selection

Programming the Enterprise Edge system for Call by Call Service Selection with a PRI interface requires:

- Provisioning a DTI as PRI if a DTI configured as PRI is not already a part of the system, see the Maintenance section.
- Selecting a protocol, on page 99.
- Programming incoming call routing, on page 152.
- Programming routes that use the PRI pools, see Call Routing on page 128.

CbC limits

PRI pool limits for Call by Call services allows you to configure limits for service types without interacting with the CO. This feature sets the minimum and maximum number of incoming and outgoing calls per service type for the PRI pool.

The number of active calls will be tracked and whenever a call is being setup, a check will be made to determine if it will be allowed. Calls will not be allowed if they exceed the maximum value for that service type or if they will use lines needed to maintain the minimum value of other service types.

The summation of the minimum values for incoming or outgoing PRI services cannot exceed the total number of lines in the PRI pool.

The maximum value for an incoming or outgoing PRI service cannot exceed the total number of lines in the PRI pool.

Programming CbC limits

1. From **General Settings, CbC limits**, select a pool (PRI-A to PRI-F) that supports Call by Call routing.

2. Select a service.
   The services that display depend on the protocol.

3. Type a number if required under **Min incoming:2**.

4. Type a number if required under **Max incoming:23**.

5. Type a number if required under **Min outgoing:4**.

6. Type a number if required under **Max outgoing:23**.

Line Pools

All lines in a PRI interface are in the same PRI line pool. This pool cannot contain any non-PRI lines. There is one PRI pool available for each PRI interface. Depending on the order that the modules are configured as PRI, Pool PRI-A represents lines 061 to 083, Pool PRI-B represents lines 085 to 107, and Pool PRI-C represents lines 109 to 131, etc. to Pool PRI-F. If all PRIs are connected to the same service provider and use the same protocol, lines 061 to 083, 085 to 107, and 109 to 1311 etc. can be put in the same pool, PRI-A, PRI-B, PRI-C up to PRI-F.

Release reasons

This setting is useful for diagnostic purposes. It shows the reason why an ISDN call is released. The Release reasons can display as Simple or Detailed text. When the default **None** is selected, no release reason appears on the set.

1. Select **Services**, **Telephony Services**, **General settings**, **Release reasons**.

2. Choose a Text setting: **Simple**, **Detailed,** or **None**.

Note: If you select **Simple** text, you must disable the **Cause code**. This is for diagnostics.

Network Services

Network Services allows you to configure access to outside the network.

ETSI

You can allow users to redirect calls on an ETSI ISDN line to outside the network.

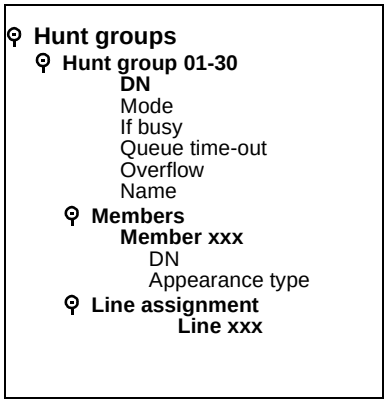
To allow Network Diversion:

1. Select **Services**, **Telephony Services**, **General settings**, **NetworkServices**, and click on the **ETSI** heading.

2. In the **NetwkDiversion** box, select **Y**.

Hunt groups

The Hunt groups heading allows you to assign a group of Enterprise Edge sets to a Hunt group. A single directory number ensure that calls route to the appropriate Hunt group. The following shows a detailed view of the Hunt groups programming map.



You can create a Hunt group for a group of persons performing the same task, and answering a number of related telephone queries. Some typical uses of Hunt groups are:

- a sales department answering questions on product prices or availability
- a support department answering questions concerning the operation of a product
- an emergency department answering calls for help

You can use Hunt groups to route calls to a support service such as a Help Line for a software company. Specialists handling Product A can be in one group, and specialists handling Product B can be in another group. Incoming calls hunt for the next available set in the group. If no set is available, the system places the call in a queue or routed to an overflow set.

In the Hunt groups subheading you can program the following:

- members of a group
- member position in a group
- what lines you assign to a group
- how the system distributes incoming calls
- how long the system looks for available members
- where a call goes if all members are busy

Note: Do not program videophones as members of a Hunt group. Hunt groups allow one B channel connection at a time and videophones use two B channels.

The operation of some features varies if the Enterprise Edge set is part of a Hunt group. The table below shows the affected Features.

Feature	Description
Call Forward All Calls	The system ignores Call Forward All Calls feature and the Hunt group call rings at the set.
Call Forward No Answer	The system ignores Call Forward No Answer and the Hunt group call continues to ring until the hunt time expires.
Call Forward on Busy	The system ignores Call Forward on Busy and the Hunt group call continues to ring until the hunt time expires.
Do not Disturb on Busy	If this feature is active, the set will not receive notification of incoming Hunt group calls.
Group Pickup	If a set is part of a Hunt group and a call pickup group, then an incoming Hunt group call can be picked up from any set that is in the call pickup group.
Transfer via Hold	The system support transfer for Hunt group sets; however, you cannot Transfer via Hold. Once you answer a call on a Hunt group set, its appearance disappears from all other sets in the Hunt group so that other calls can come in on the same line.
Priority Call	You cannot make Priority calls to Hunt group DNs.
Ring Again	You cannot use Ring Again when calling a Hunt group DN.
Line Redirection	The Allow redirect attribute should be set to N for lines assigned to Hunt groups. For more information, see Capabilities on page 98.
Page Zones	You cannot include Hunt group DNs in a Page zone.
Voice Call	Hunt groups cannot accept voice calls. Answer buttons have no appearances for voice calls, and the set does not ring.

Adding or removing members from a group

Any Enterprise Edge set, or portable can be a members of a Hunt group. An Enterprise Edge set can be in more than one Hunt group but is considered a member in each Hunt group, increasing the total number of members in the system.

There can be only one appearance of the same Hunt group on a set. Hunt group DNs cannot be members of other Hunt groups. A DN can be associated with a member of a Hunt group and is called a member DN.

Consult your customer service representative to determine your Hunt group number range.

To add a member to a Hunt group:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.

2. Click a Hunt group (**Hunt group 1-30**).

3. Expand the Hunt group heading and click **Members**.
4. Click the **Add** button above the navigation tree.
5. Type a number in the **DN number** box.
6. Click the **Save** button.

To remove a member from a Hunt group:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1**-**30**).
3. Expand the Hunt group heading and click **Members**.
4. Click the member (for example, Member 001) to be removed.
5. Click the **Delete** button above the navigation tree.

To remove all members from a Hunt group:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1**-**30**).
3. Expand the Hunt group heading and click **Members**.
4. Click the **Delete All** button above the navigation tree.

Moving members of a group

Member order within a Hunt group is important. The member order determines how a call routes through a Hunt group.

To move a member within a Hunt group:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (Hunt group 1-30).
3. Expand the Hunt group heading and click **Members**.
4. Click a member from the member list (for example **Member 003**).
5. On the **Configuration** menu, click **Move**.
6. Type the new member number (001, 002, etc.) in the **Move to** box.

7. Click the **OK** button.
   The system automatically reorders the list.

Assigning or unassigning lines to a group

Configure the prime set for a Hunt group's line to None to avoid delayed ring transfer of external Hunt group calls to the prime set before the Hunt group can receive the call. For more information about programming line settings, see Prime set on page 113.

You can assign a line to only one Hunt group.

To assign a line to a Hunt group:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1-30**).
3. Click **Line Assignment**.
4. Click the **Add** button above the navigation tree.
5. Type a line number (for example 061) in the **Line number** box.
6. Click the **Save** button.

To unassign a line:

1. Click a Hunt group (**Hunt group 1-30**).
2. Click **Line Assignment**.
3. Click the line number (for example, **Line 061**) to be deleted.
4. Click the **Delete** button above the navigation tree.

To unassign all lines in a Hunt group:

1. Click a Hunt group (**Hunt group 1-30**).
2. Click **Line assignment**.
3. Click the **Delete All** button above the navigation tree.

Setting the Distribution mode

There are three modes of call distribution:

- Broadcast—rings each set in the group simultaneously. Hunt group handles calls one at a time; other calls put in a queue. As soon as you pick up a call, the call next in the queue presents to the Hunt group without waiting for queue time-out.
  In Broadcast mode, a single incoming call rings simultaneously at all the sets in a group. This way, all receptionists in the group share the load of answering large volumes of calls. All sets automatically display the calling line identification (CLID), if available. A familiar example is a fund-raising campaign where a group of operators wait to take each call as it comes in.
- Linear—starts the call at the first set in the Hunt group and distribution is complete when the first free set is found. All calls present simultaneously. Distribution is order based.
  In Linear mode, you can program your top salesperson to be the first member of the Hunt group to receive incoming calls.
- Rotary—the call starts at the set after the one that answers the last call. Distribution is complete when the next free set is found. Call can present simultaneously. Distribution is order based.
  In Rotary mode, you can ensure that all your helpline people receive calls on an equal basis, rather than one person receiving the majority of calls. The call rings at one set at a time in a round-robin fashion.

If a Hunt group has available members but nobody answers the call, the call routes through the Hunt group list until either someone answers the call or the queue time-out occurs. In the latter case, the call routes to the overflow position. Once a call goes to the overflow position, it is no longer a Hunt group call.

To set the call distribution mode:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1-30**).
3. Click a Mode value **Linear**, **Rotary**, **Broadcast** and press **Enter**.

Setting the hunt delay

This setting allows you to program the number of rings the system permits at a Hunt group set before moving on to the next set in the Hunt group. This attribute appears only if the distribution mode is set to Linear or Rotary. For more information, see Setting the Distribution mode on page 174.

1. Choose **Services**, **Telephony Services**, **Hunt Groups**.
2. Click a Hunt group (**Hunt group 1-30**).
3. Click a Hunt Delay value **1** to **10** and press **Enter**.

Programming busy line setting

A Hunt group is busy if one of two scenarios exists:

- An incoming Hunt group call presents to all of its members.
- All of its members are active on a Hunt group call.

There are three routing options if a Hunt group is busy:

- Busy tone—the caller gets a busy tone (PRI lines only).
- Overflow—the call routes to an overflow position. If the overflow DN is the hunt group DN for that same Hunt group, the overflow option does not appear.
- Queue—the call stays in the system for a period of time. Within this period of time, the call presents to a member if one becomes available. When time-out occurs, the call presents to an overflow position.

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1**-**30**).
3. Click an If Busy value: **Busy tone**, **Overflow**, or **Queue**, and press **Enter**.

Queue time-out

This setting allows you to program the number of seconds a call remains in the Hunt group queue before it routes to the overflow position.

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1**-**30**).
3. Click a Queue timeout value: **15**, **30**, **45**, **60**, **120**, or **180** and press **Enter**.

Overflow set

The Overflow setting allows you to program the overflow set where unanswered Hunt group calls go. Unless the overflow position is a Hunt group set, the call is no longer a Hunt group call. If the overflow set is a Hunt group set, Enterprise Edge considers the call as a new call and it goes to the bottom of the queue.

The overflow set can be a set DN number associated with a voice mailbox:

1. Choose **Services**, **Telephony Services**, **Hunt groups**.
2. Click a Hunt group (**Hunt group 1**-**30**).
3. Type the DN number in the **Overflow** box, and press Enter.

Name

The Name setting allows you to program the Hunt group name, such as SERVICE or SALES. The name can be up to seven characters in length.

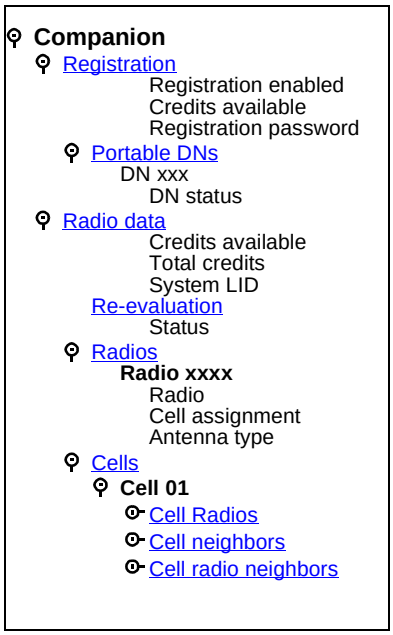
1. Choose **Services**, **Telephony Services**, **Hunt groups**.

2. Click a Hunt group (**Hunt group 1**-**30**).

3. Type a new name and press **Enter**.

Companion

The Companion heading allows you to assign portable telephones to the system, check Base Station parameters, and enable and disable registration through programming. The following illustration shows a detailed view of the Companion programming map.



Note: Enterprise Edge Companion Wireless requires a software keycode to activate.

Registration

Software Keys are required to activate wireless capabilities.
To take advantage of the wireless capabilities available to your Enterprise Edge system, you must first enable a certain number of portable credits using Software Keys.

You must enable registration for the entire Enterprise Edge system to allow registration of individual portables.

To enable user registration:

1. Select **Services, Telephony Services**, **Companion**, **Registration**.
2. Select a **Registration enabled** option: **Y** (Yes) or **N** (No).
3. Press **Enter**.

Registration should normally be disabled.
For security reasons, and to prevent unauthorized users from being registered to your system, disable Registration when you have finished registering the portables.

Changing the Registration password

To ensure that no one registers unauthorized portables to your system, there is a separate level of password access. You can, and should, set your own password to prevent unauthorized handsets from registering on your system.

Change password to avoid incorrect registration.
To ensure accurate registration, change the Registration password before registering any portables. If there is another wireless system in radio range, and both systems have the same Registration password and Registration enabled, you may accidentally register on the other system instead of on your own.

The default Registration password is 72346.

To program a new Registration password:

1. Select **Services, Telephony Services**, **Companion**, **Registration**.

2. Type a new password in the **Registration password** box.

Tip
You can choose any combination of one to six digits. It is easier to remember the password if the digits spell a word. Provide this password only to selected personnel to prevent unauthorized access to programming. The implications of such access may include the rearrangement of line assignments, which could affect the operation of Enterprise Edge.

Portable DNs

Once you enable registration for your Enterprise Edge system, a series of extension numbers (469 to 500) are automatically available for registration. Check that an extension number is available before registering a portable telephone to it.

If the extension number shows a status of Available, it is ready for registering a Companion portable telephone.

If the extension number shows a status of Registered, a Companion portable telephone is already registered to that extension number. In this case, you can either pick a different extension number, or deregister the current portable telephone. You must perform deregistration both at the portable and from Unified Manager.

To view registered and available DNs:

1. Select **Services, Telephony Services**, **Companion**, **Registration**, **Portable DNs**.

2. Click a portable DN (for example, DN 471).
   The **DN status** box appears.

Deregistering a portable

Deregister an extension number from Unified Manager when:

- You must replace the portable due to loss or breakage.
- You want to assign the handset to someone with a different telephone number than the previous user.

To deregister a portable:

1. Select **Services, Telephony Services**, **Companion**, **Registration**, **Portable DNs**.

2. Click a portable DN (for example, **DN 471**).
   The DN status window appears.

3. On the **Configuration** menu, click **Deregister**.

Tip
This procedure does not clear the registration data in the portable. You must also deregister from the portable telephone ("on-the-air" deregistration).

Radio data

The Radio data heading allows you to view the number of credits available, the total number of credits and the System LID.

1. From **Companion**, click on the **Radio data** heading.
   The Radio data window appears.

Re-evaluation

Re-evaluation automatically assigns the proper cell configuration to each radio in a Base Station. When you add or remove Base Stations, you must apply Re-evaluation to the system.

If the Re-evaluation status reads **Required**, you can carry out the re-evaluation.

To view the Re-evaluation status:

1. Select **Services, Telephony Services**, **Companion**, **Radio data**.

2. Click **Re-evaluation**.

3. On the **Configuration** menu click **Re-eval now** or **Schedule**.

Radios

The Radios setting allows you to program Base Stations settings.

Cell assignment

A cell is the area covered by one or more radios in close proximity. As you move around your office while on a call with your portable, the call hands off from one cell to another. A call on a portable hands off from one cell to another only if Enterprise Edge assigns those cells as neighbors. Enterprise Edge automatically assigns cell neighbors and re-evaluates the cell-to-cell configuration when you add or remove Base Stations.

The cell assignment setting allows you to see if a Base Station radio is assigned to a cell in the Companion system.

To view the cell assignment:

1. Select **Services, Telephony Services**, **Companion**, **Radio data**, **Radios**.

2. Click **Radio nnnn**. Where **nnnn** is the four-digit radio number.
   The Radio screen appears. The **Radio** box displays the radio number. The **Cell assignment** box appears if the radio is Assigned or Unassigned.

3. In the **Antenna type** box select if the radio antenna is **Internal** or **External**.

Cells

Cell programming allows you to examine the cell radio, cell neighbor, and cell radio neighbor settings.

1. Select **Services, Telephony Services**, **Companion**, **Radio data**, **Cells**.

2. Select a cell number (**Cell 01** to **Cell 32**).

Cell Radios

The Cell radios subheading allows you to view the 5-digit number of any radios assigned to this cell. For example, if radio 07012 is in the cell, 07012 assigned appears.

1. Select **Services, Telephony Services**, **Companion**, **Radio Data**, **Cells**, **Cell nn**, **Cell radios**.

2. Click on the radio number to view the setting: **Assigned** or **Unassigned**.

Cell neighbors

The Cell neighbors subheading allows you to view the 2-digit number of any cells that border a particular cell in a system.

1. Select **Services**, **Telephony Services**, **Companion**, **Radio Data**, **Cells**, **Cell nn**, **Cell neighbors**.

2. Click on the cell number to see the settings: **Assigned** or **Unassigned**. For example, cell 01, Neighbour:03 and Neighbour:04 display. This means that cells 03 and 04 are assigned as cell neighbors.

Cell radio neighbors

The Cell radio neighbors subheading allows you to view the 2-digit number of any cells that border a particular cell in a system (the cell neighbors) plus any cells that border the cell neighbors.

1. Select **Services**, **Telephony services**, **Companion**, **Radio Data**, **Cells**, **Cell nn**, **Cell radio neighbors**.

2. Click on the cell number to see the settings: **Assigned** or **Unassigned**. For example, cell 01, Radio neighbour:03, Radio neighbour:04 display, and Radio neighbour:11. Cell 11 does not appear as a cell neighbor (see the example under Cell neighbor), therefore it must be a neighbor of cell 03 or 04.

Register individual portables

You must do two things to register each portable with Enterprise Edge:

- Register the portables by entering the Registration password on each one.
- Verify that the portable operates properly.

When you distribute the portables, tell the users that the portables are registered and give them the corresponding extension numbers.

Tip

You can register a portable to more than one system. You cannot register a portable to more than one extension number per system. You cannot register more than one portable to one extension number.

If a portable telephone is to be used in more than one Enterprise Edge system, its owner must know which registration slot number was used to register the portable telephone with each system. (It is preferable that each user have the system they use most often registered in slot 1.)

If a portable telephone is lost or broken, deregister it from the system before replacing it with another portable telephone.

Portable telephone programming

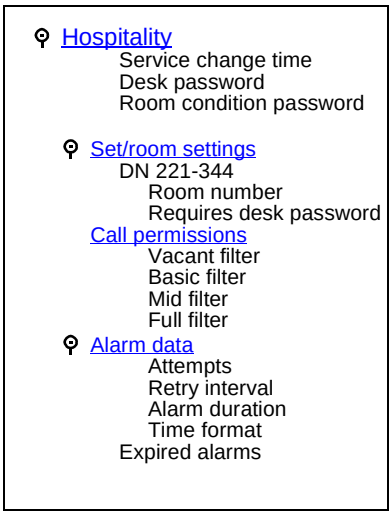
Once the registration process is complete, portable telephone programming is much the same as it is for Enterprise Edge desk telephones. Some of the programming settings do not affect the operation of the portable.

The table below shows the recommended settings for Enterprise Edge.

Programming level	Programming option	Setting	Notes
Terminals & sets/ Capabilities	Forward no answer	Fwd to: <DN> Fwd Delay: <no. of rings>	This stops the Companion portable from ringing when the call has been forwarded to its new destination. The portable user can still answer the call, but it does not ring. The settings for Forward no answer are found under **Terminals & sets, Capabilities** in the Unified Manager.
	Forward on busy	Y	
	Do not disturb on busy	N	
	Handsfree	N	
	Handsfree answerback	None	
	Pickup group	<group number>	A portable can be part of a pickup group and answers calls ringing at telephones in the same group when the user enters *76. (See Capabilities on page 98 for more information about Group pickup.)
	Paging	Y	
	Page zone	1	
	Direct dial	Set 1	A portable cannot be a Direct dial telephone. It can use the Direct dial digit.
	Hotline	None	
	Priority call	Y	Requires special configuration of hardware and programming
Terminals & sets/ Restrictions/Set Restrictions	Set lock	Y	Does not apply to portables.
	Allow last number	Y	Does not apply to portables.
	Allow saved number	Y	Does not apply to portables.
	Allow link	Y or N	This can be set to N for portables.

Hospitality

Hospitality Services (HS) is a group of features that increases the value of the Enterprise Edge system in small- to medium-sized facilities such as hotels, motels or hospitals. The following illustration shows a detailed view of the Hospitality programming map.



In a hotel setting, guests gain improved services through immediate access to basic functions like:

- Wake-up service or reminders
- Accurate tracking of the room's service requirements

The system classifies Enterprise Edge telephones as one of three types of sets: a common set, a room set or a Hospitality Services (HS) admin set.

Common set

A common set can be a telephone found in a lobby, office, or common area. It is not associated with a room and does not have access to all of the HS features.

Common sets are Enterprise Edge telephones or analog telephones connected to an analog terminal adapter (ATA), or an analog station module (ASM).

Room set

A Room set is a set you assign to a room. You can assign up to five sets to the same room (they all share same room number).

Room sets can be any Enterprise Edge telephone or an analog telephone connected to an ATA or an ASM.

Hospitality Services (HS) admin set

A Hospitality Services (HS) admin set is any two-line display Enterprise Edge telephone. You can program an HS admin set to require you to enter the Desk admin password before the system grants access to HS administrative features.

Alarm time (AL) feature

The Alarm time feature provides an alarm clock capability on Enterprise Edge and analog telephones that connect to an ATA or an ASM. You can program both room sets and common sets to sound an audible alert at time you request.

You can program one Alarm time within a 24 hour period on a room or common set and you must reset the alarm daily. When the alarm sounds, all sets in a given room alert. When you cancel the alarm on any set cancels the alarm on all the sets in the room. A new Alarm time entered on a room or common set overwrites any alarm set previously.

If the Enterprise Edge system experiences a power failure, the failure can result in lost Alarm times. When the Enterprise Edge system is running and the system's time resets, the missed Alarm times alert. At all times, the Enterprise Edge system allows up to a maximum of 25 sets that can alert at the same time.

For more information about programming this feature, see the *Enterprise Edge Feature Telephone Programming Guide*.

Service change time

The Hospitality setting allows you to enter the time when occupied rooms change state from Service done to Service required. The Service change time is an primary part of the Room condition (RC) feature.

To change the service time:

1. Choose **Services**, **Telephony Services**, and click on the **Hospitality** heading.

2. Type the time in the **Service change time** box according to the following format and press Enter:
   hh is a number from 00 to 23
   mm is a number from 00 to 59

Desk password

The Desk password setting controls access to all Hospitality Services administrative features. The default Desk password is 4677. It is recommended that you change the password to prevent unauthorized use.

To change the Desk password:

1. Choose **Services**, **Telephony Services**, and click on the **Hospitality** heading.

2. Type a password (1 to 6 digits) in the **Desk password** box and press **Enter**.

Room condition password

The Room condition password setting controls access to the Room condition feature (Feature 8 7 6). The default Room condition password is **None**. For more information about using Feature 8 7 6 , see the *Enterprise Edge Feature Telephone Programming Guide*.

To create a Room condition password:

1. Choose **Services**, **Telephony Services**, and click on the **Hospitality** heading.

2. Type a password (1 to 6 digits) in the **Room condition password** box, and press **Enter**.

Set/room settings

The Set/room settings allows you to assign sets to a room and enable access control to HS administrative features.

To assign a set to a room:

1. Choose **Services**, **Telephony Services**, **Hospitality**, **Set/room settings**.

2. Click a DN number (DN 221-344).

3. Type a room number in the **Room number** box, and press **Enter**.

To enable or disable password control:

1. Choose **Services**, **Telephony Services**, **Hospitality**, **Set/room settings**.

2. Click a DN number (DN 221-344).

3. Click a **Requires desk password** value: **Y** or **N**, and press **Enter**.

   The default setting is **Y**. This means that you cannot access administrative features from a room set without first entering a valid password. You can define a Desk password under the Hospitality heading. For more information, see Desk password on page 184.

Call permissions

The Call permissions heading allows you to assign dialing filters to room sets based on the room occupancy status. The Vacant state indicates that the room is empty. The Basic, Mid and Full states indicate that the room is occupied. The default dialing filter for all Room occupancy states (Vacant, Basic, Mid, and Full) is **00**. The dialing filters are standard Enterprise Edge Restriction filters (Filters 00-99). For more information, see Restriction filters on page 124.

To assign dialing filters:

1. Choose **Services**, **Telephony Services**, **Hospitality**, and click on the **Call permissions** heading.

2. Type a 2-digit filter number in the **Vacant**, **Basic**, **Mid** or **Full filter** boxes, and press **Enter**.

Alarm data

The Alarm data heading allows you to program the following alarm settings:

- Attempts - the number of times the Alarm time feature attempts to alert the occupant before cancelling.
- Retry interval - the interval period in minutes between each attempt.
- Alarm duration - the period in seconds that a set alerts for each alarm attempt.
- Time format - the hour format used, 12-hour or 24-hour.

To define the Alarm Data:

1. Choose **Services**, **Telephony Services**, **Hospitality**, and click on the **Alarm data** heading.

2. Click an **Attempts** value: **1** to **5**, and press **Enter**. The default value is **3** attempts.

3. Click a **Retry interval** value: **2** to **9**, and press **Enter**. The default value is **4** minutes.

4. Click an **Alarm duration** value: **10**, **15**, **20**, **25**, **30**, **35**, **40**, **45** or **50**, and press **Enter**. The default value is **15** seconds.

5. Click a **Time format**: **12 hour** or **24 hour** and press **Enter**.

Expired alarms

The Expired alarms setting allows you to program the system to notify a set when a Hospitality alarm expires. You can also program whether a caller hears a tone when an alarm expires.

1. Choose **Services**, **Telephony Services**, **Hospitality**, **Alarm data**, and click on the **Expired alarms** heading.

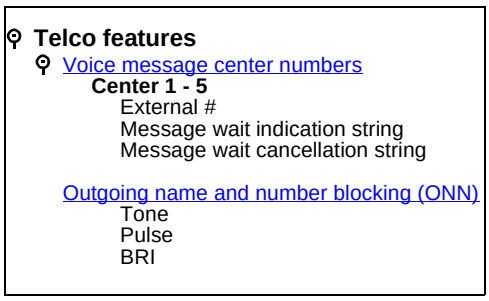
2. In the **Notify set** box select: **None** or **DN:**.

3. If you select **DN:**, type in the DN number that you want to notify when an alarm expires.

4. In the **Use tone** box select **Y** or **N**.

Telco features

The Telco features heading allows you to define settings for voice message center numbers and outgoing name and number blocking. The following illustration shows a detailed view of the Telco Features navigation tree.



Voice message center numbers

If you subscribe to a voice message service outside your office, you can access it through your Enterprise Edge system. You can specify what voice message center you use for each external line that receives message waiting indication. This setting specifies the external telephone numbers that the Message feature dials to retrieve voice messages.

1. Choose **Services**, **Telephony Services**, **Telco features**, and expand **Voice message center numbers** in the navigation tree.

2. Click on the Center number you want to program. For example, **Center 1**. The Center 1 screen appears.

3. Enter the **External #** for up to five message centers: Center 1 through Center 5. The default for each voice message center number is an empty box.

Tips

A telephone does not show that external voice messages are waiting unless you enable External voice message set. The setting is in under **Terminals & sets, Line access, Line assignment**.

You can program up to five voice message center numbers, but many systems require only one.

DPNSS settings

- **Message wait indication string (AN*1#)**: indicates that the message center has a message in the mailbox. This is a default NSI string for message waiting.
- **Message wait cancellation string (AN*0#)**: indicates that the voice mails have been retrieved. Again, this is a default NSI string for message waiting.

Outgoing name and number blocking (ONN)

The Outgoing name and number blocking feature blocks the outgoing name and number on a per call basis. When you use this feature, the system flags the call to the CO so that the name and number does not present to the person you call. See Outgoing name and number blocking (ONN) on page 186 for more information.

1. Choose **Services**, **Telephony Services**, **Telco features**, **ONN blocking**.

2. Enter the telephone number for ONN blocking in the **Tone**, **Pulse**, or **BRI** boxes.

Voice Mail

For information on Voice Mail service configuration, refer to the following documents:

- *Enterprise Edge 2.0 Voice Messaging Set Up and Operation Guide*
- *Enterprise Edge 2.0 Voice Messaging Reference Guide*
- *Enterprise Edge 2.0 Voice Messaging Quick Reference Guide*
- *Enterprise Edge 2.0 Voice Messaging Programming Record*
- *Enterprise Edge 2.0 AMIS Set Up and Operation Guide*
- *Enterprise Edge 2.0 AMIS User Guide*
- *Enterprise Edge 2.0 Networking Set Up and Operation Guide*
- *Enterprise Edge 2.0 Networking User Guide*
- *Enterprise Edge 2.0 FAX Set Up and Operation Guide*
- *Enterprise Edge 2.0 FAX User Guide*
- *Enterprise Edge 2.0 Unified Messaging Client Installation Guide*
- *Enterprise Edge 2.0 Unified Messaging Quick Reference Guide*
- *Enterprise Edge 2.0 Call Center Set Up and Operation Guide*
- *Enterprise Edge 2.0 Call Center Agent Cards*
- *Enterprise Edge Call Center Reporting Set Up and Operation Guide*

Call Detail Recording

For information on Call Detail Recording, refer to the *Enterprise Edge Call Detail Recording System Administrator Guide*.

TAPI

For information on TAPI Service Provider, refer to the *Enterprise Edge 2.0 TSP Server Configuration Guide*.

Console Service

For information on Console Service, refer to the *Enterprise Edge 2.0 Attendant Console Set Up and Operation Guide* or the *Enterprise Edge 2.0 Attendant Console User Guide*.

VoIP Gateway

The Voice over IP (VoIP) Gateway settings allow you to configure the Local (H323) and Remote Gateways for Enterprise Edge.

To view and change the status of VoIP gateway settings:

1. Choose **Services**, and click on the **VoIP Gateway** heading.
   The VoIP Gateway Summary screen appears.

2. View the VoIP Gateway Summary attributes and configure the status according to the table below:

Attribute	Description
Description	Shows the description of the VoIP gateway.
Version	Shows the version of the VoIP gateway.
Status	Allows you to choose **Enabled**, **Disabled**, **Paused**, or **Continue** for the VoIP gateway service.

3. Press the **Tab** key to save the settings.

VoIP local and remote gateways

To configure VoIP local and remote gateways:

1. Choose **VoIP Gateway** and click on **H323 Gateway** heading (Local).
   The Local Gateway screen appears.

2. Configure the VoIP Local Gateway attributes according to the table below:

Attribute	Description
Preferred Codecs 1st to 5th	Allows you to specify the local VoIP gateway to convert voice to data packets and vice versa. The system negotiates these parameters during call setup with the other VoIP gateway involved in the call. Enterprise Edge negotiates Codecs in the order of preference you specify here. Refer to the *VoIP Gateway User Guide* for a discussion on these values.
Echo Cancellation	Allows you to enable or disable the Echo Cancellation feature in the VoIP calls.
Non-linear Processing	Allows you to enable or disable non-linear processing.
Silence Compression	Allows you to enable or disable silence compression.

Attribute	Description
Fallback to Circuit Switched	Allows you to enable or disable fallback to the circuit switched network (PSTN).
Voice Jitter Buffer	Allows you to specify the voice jitter buffer size in the range of 20-200. The default setting is 50. Press the **Tab** key.
Fax Jitter Buffer	Allows you to specify the FAX jitter buffer size in the range of 20-200. The default setting is 50. Press the **Tab** key.
Local Gateway IP	Allows you to specify the local VoIP gateway IP Address when Enterprise Edge interacts with other VoIP gateways. Since the Enterprise Edge server typically has more than one IP interfaces and more than one IP Address, you must choose one that the VoIP gateway uses. This address must match the entry for this gateway in the remote gateway table of those VoIP gateways. Ensure other gateways can reach this address via IP. For example, IP-LAN1. Press the **Tab** key.
Gatekeeper	Allows you to specify the IP address for an external gatekeeper. Set this to None if the gatekeeper functions locally. The default is **None**.
Call Signaling	Allows you to specify how directory numbers convert into the destination IP address. **Direct**: gateway resolves addresses locally using the remote gateway table. **GatekeeperRouted**: gateway sends call signaling messages to the gatekeeper. You must set Gatekeeper parameters to support this. **GatekeeperResolved**: gateway uses endpoint location services of the external gatekeeper to resolve addresses before sending call signaling directly to destination. This is not supported in release 2.0. The default is **N/A**.
Alias Names	Allows you to enter the text name that Enterprise Edge uses to register with the Gatekeeper. This identifies the H323 (Local) gateway. The default is **N/A**.

3. Press the **Tab** key save the settings.

Remote Gateway

To add remote gateways:

1. Choose **VoIP Gateway**, and click on the **Remote Gateway** heading.
   The Remote Gateway list appears.

2. On the **Configuration** menu, click **Add Entry**.
   The Remote Gateway screen appears.

3. Configure the VoIP Remote Gateway attributes according to the table below:

Setting	Definition
Name	Allows you to specify a logical name for the remote VoIP gateway. You can edit this setting only when you add a new gateway entry. While you modify an existing entry, this name cannot be changed.
Destination IP	Allows you to specify IP Address for the remote VoIP gateway. You can enter a fully qualified DNS Name or just host name (where applicable) or IP address in dotted format. Press the **Tab** key.
QoS Monitor	Allows you to enable or disable QoS Monitor for this VoIP gateway.
Transmit Threshold	Allows you to specify the transmit threshold while interacting with this VoIP gateway. Press the **Tab** key.
Receive Threshold	Allows you to specify the receive threshold while interacting with this VoIP gateway.
Gateway Type	Allows you to specify the VoIP gateway type. VoiceNet is the only permitted value in Release 2.0.
Destination Digits	Allows you to specify the destination digits for this gateway. When the local gateway sees this prefix, it forwards the call to the VoIP gateway at the specified destination IP Address. Press the **Tab** key.

4. Click the **Save** button.

To modify remote gateways:

1. In the **Remote Gateway** table, click the remote gateway you want to modify.

2. On the **Configuration** menu click **Modify Entry**.
   The Remote Gateway screen appears.

3. Modify the Remote Gateway attributes.

4. Click the **Save** button.

To delete remote gateways:

1. In the **Remote Gateway** table, click the remote gateway you want to delete.

2. On the **Configuration** menu, click **Delete Entry**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion.

DHCP

Enterprise Edge provides DHCP (Dynamic Host Configuration Protocol) service to branch office clients. This service dynamically assigns IP addresses to branch office PCs, so you do not need to manually assign an IP address to each PC.

To configure Enterprise Edge as your DHCP server, you must create a scope of IP addresses for each LAN interface and then allocate a block of IP addresses to that scope. If you already have a DHCP server then you need to set up Enterprise Edge as a relay agent to that server.

Tips

Because Enterprise Edge retrieves default DHCP parameters from the LAN interface parameters, you must configure a LAN interface before you configure the DHCP server for that interface. For information on configuring a LAN interface, see LAN1 on page 47.

You must define one DHCP scope for each LAN interface. For DHCP service, there are global attributes that affect all scopes, and there are attributes that are specific for each scope.**r**

Tip

Use Enterprise Edge DHCP default configuration unless your network does not allow it.

If you must modify the DHCP default configuration on Enterprise Edge, make sure configuration settings are consistent throughout the network and take the following into consideration:

- If a change in the DHCP configuration resulted in a change in the ‘Router’ and ‘Subnet mask’ fields for a given scope of IP addresses, perform one of the following actions to ensure good system operation:

  - Execute *ipconfig/release* and *ipconfig/renew* on each of the workstations. For Windows 95 and Windows 98, use the *winipcfg*.

  - For clients that do not support *ipconfig* and *winipcfg*, a reboot is necessary to renew their IP addresses.

- If you made a change in the DNS server configuration or DNS name field, repeat the actions stated in step 1 above to ensure proper connectivity with the network.
- Always schedule a down time when making changes to the Enterprise Edge DHCP server configuration to minimize impact on your network users.
- Reboot the Enterprise Edge system for the changes to take effect.

To configure global attributes for DHCP:

1. On the navigation tree, choose **Services** and click on the **DHCP** heading to view the Mode, Global Options and Summary screens for DHCP.

2. Select the DHCP mode, **DHCPRelayAgent** or **DHCPserver**.

Configuring a DHCPServer

3. Configure the settings in the DHCPServer Global Options and DHCP Summary screen:

Setting	Definition
IP Domain Name	This setting defaults to the value entered in the **Domain** box of the DNS Summary page (see DNS) because all the DHCP clients of an Enterprise Edge server are in the same DNS domain as the Enterprise Edge server. Enterprise Edge runs only a DNS cache and does not introduce another DNS zone. The domain name is passed to the client when Enterprise Edge responds to a client's DHCP requests. Use caution if you change this.
WINS Node Type	Allows you to specify a clients WINS node type. Enterprise Edge automatically sets this value to **8** (indicating H-Node) on all DHCP clients of Enterprise Edge. This setting configures the DHCP client PCs to use p-node name resolution before resorting to b-node name resolution, which is efficient when a WINS server is configured for the network. Enterprise Edge also includes a WINS server. Other options available are: **1**: indicates a b-node that uses broadcast mechanism for NetBIOS name resolution. **2**: indicates a p-node that uses point-to-point mechanism involving a WINS Server for NetBIOS name resolution. **4**: indicates a m-node that first uses broadcast and then point-to-point mechanism for NetBIOS name resolution. Use caution if you change this.
Description	Provides a description of the Enterprise Edge server.
Version	Shows the version number of the Enterprise Edge server.
Status	Allows you to enable or disable the DHCP server. When you disable the server, you need to assign static IP addresses to clients.

4. Press the **Tab** key to save the settings.

Configuring a DHCPRelayAgent

If you choose DHCPRelayAgent as the mode, the Global Options screen and Server List appear and the Configuration menu is enabled.

1. Choose what the log displays, **Errors Only**, **Warnings Also**, **Maximum** or **Disabled**. The default is **Errors Only**.

2. On the **Configuration** menu, click **Add server**.
   The Server list dialog box appears.

3. Type in the IP Address of the server.

   Note: You can specify a number of servers. The routing component searches the list for the server on the same subnet as the interface and forwards the packet.

4. Click **Save**.

LAN settings for DHCPServer

If you configured the DHCP mode for DHCPServer in the previous procedure then configure LAN1 scope attributes as follows. If the mode is DHCPRelayAgent refer to LAN settings for DHCPRelayAgent on page 198.

1. Choose **Services**. Click the **DHCP** navigation key to expand the navigation tree.

2. Click on the **LAN1** heading.

   Note: If your Enterprise Edge system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1, LAN2, etc. This section describes configuring the DHCP scope for LAN1. Follow the same instructions to configure any of the parameters under the scope for LAN2.

   The frame displays the LAN Scope Specific Options, Address Range, and Excluded Address Range screens.

3. Scroll down to view all settings.

4. Configure the scope-specific settings. Refer to the DHCP LAN attribute table below.

5. Configure the LAN address range and the LAN excluded address services screens through the menu. Refer to the DHCP LAN attribute table below.

Note: If the IP Address or subnet mask for a LAN interface changes, the system creates or modifies the corresponding DHCP scope for the interface. This operation also involves setting default values for some parameters. By default, Enterprise Edge sets the IP Address of corresponding LAN interface to DNS Server, WINS Server, Default Gateway options of the scope. It also sets the lease time to 3 days and creates a range of addresses for the scope. If the IP Address of the LAN interface is in the lower half of the subnet, the address range set for the scope includes all the address above the LAN interface address. If the IP Address of the LAN interface is in the upper half of the subnet, the address range set for the scope includes all the address below the LAN interface address. By default, the scope is enabled.

The DHCP LAN1 Scope Specific Options, Address Range and Excluded Address Range attributes are:

Attribute	Description
DNS Server	Allows you to specify the DNS server. Enterprise Edge automatically assigns the value for this parameter. If the IP Address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
WINS Server	Allows you to specify the WINS server. Enterprise Edge automatically assigns the value for this parameter. If the IP Address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
Default Gateway	Allows you to specify the default next-hop router. Enterprise Edge automatically assigns the value for this parameter. If the IP Address or subnet mask for the corresponding LAN interface changes, this value is overwritten. Use caution when changing this value.
Lease Time	Allows you to specify the time, in seconds, for an address assignment until the client's lease expires.
Scope Status	Allows you to enable or disable the scope.
Address Range	Allows you to specify the valid IP addresses for DHCP clients.
Excluded Address	Allows you to specify IP addresses that are not available to DHCP clients.

Tips

When DNS is disabled in Enterprise Edge, this box must be set to a remote DNS server.

6. Press the **TAB** key to save the settings.

To modify, add, or delete a DHCP address range or excluded address range, assign only one IP Address range for a DHCP Scope and exclude ranges of addresses in it from being assigned to clients.

To modify address ranges:

1. Click an address in the address range table.

2. On the **Configuration menu,** click **Modify Address Ranges**.
   The Address Range dialog box appears.

3. Type the necessary changes in the fields.

4. Click the **Save** button to save the modifications.

To add an address range:

1. On the **Configuration** menu, click **Add Address Range**.
   The Address Range dialog box appears.

2. In the **Range** box, type the range identifier.
   The range box uniquely identifies a range value in the scope. The value for this setting must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing range name, it modifies the existing range. If you use nonsequential numbers the system automatically reassigns sequential numbers. When you modify a range, you cannot change the range name. The range name does not have any significance other than identifying an entry.

3. In the **Start Address** box, type the start address.

4. In the **End Address** box, type the end address.
   Scroll down to see all setting fields.
   Make sure the start address and end address are in the same subnet.

5. Click the **Save** button to save the address range.

To delete an address range:

1. Click an address in the **Address Range** table.

2. On the **Configuration** menu, click **Delete Address Ranges**.
   A dialog box appears asking you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion.

   Note: When you delete or modify an IP Address range it removes any excluded addresses that are in the original address range value.

To modify excluded address ranges:

1. Click an excluded address in the **Excluded Address Range** table.

2. On the **Configuration** menu, click **Modify Excluded Address Ranges**.
   The Excluded Address Range dialog box appears.

3. Type the necessary changes.

4. Click the **Save** button to save the modifications.

To add excluded address ranges:

1. On the **Configuration** menu, click **Add Excluded Address Range**.
   The Excluded Address Range dialog box appears.

2. In the **Range** box, type the range identifier.

   Note: The range setting uniquely identifies an excluded range value in the scope. The value for this setting must follow certain conventions. You must type the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. Specify nonrecurring values for the unique number. If you specify an existing excluded range name, the system modifies the existing range. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify an excluded range, you cannot change the range name. The excluded range name does not have any significance, other than uniquely identifying an entry.

3. In the **Start Address** box, type the start address.

4. In the **End Address** box, type the end address.
   Scroll down to see all setting fields.

   Note: Make sure the start address and end address are in the same subnet, and an excluded address range is completely contained in an IP address range specified for the subnet.

5. Click the **Save** button to save the excluded address range.

To delete an excluded address range:

1. Click an excluded address in the **Excluded Address Range** table.

2. On the **Configuration** menu, click **Delete Excluded Address Ranges**.
   A message prompts you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion.

LAN settings for DHCPRelayAgent

If you configured the DHCP mode as DHCPRelayAgent (refer to Configuring a DHCPRelayAgent on page 194), then configure LAN1 scope attributes as follows. If the mode is DHCPServer refer to LAN settings for DHCPServer on page 194.

1. Choose **Services**. Click the **DHCP** navigation key to expand the navigation tree.

2. Click on the **LAN1** heading.

   Note: If your Enterprise Edge system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1, LAN2, etc. This section describes configuring the DHCP scope for LAN1. Follow the same instructions to configure any of the parameters under the scope for LAN2.

   The window displays the Relay DHCP packets, Hop-count threshold, and Seconds-since-boot threshold parameters.

Configure the scope-specific settings. Refer to the DHCP LAN Relay Agent Interface Parameters table below:

Attribute	Description
Relay DHCP packets	Allows you to enable or disable the relay of DHCP packets on this interface. Enterprise Edge automatically disables this function for each interface.
Hop-count threshold.	Allows you to specify the maximum number of hops. After this number of hops, DHCP requests are discarded. The values are 0 to 16. The default value is 4.
Seconds-since-boot threshold	Allows you to specify the minimum number of seconds since the last boot, before Enterprise Edge forwards DHCP requests. The values are 1to 3600. The default value is 4.

3. Press the **Tab** key to save the settings.

DNS

Enterprise Edge functions as both a gateway to the Internet and as a DNS proxy.

Note: If your PC is a DHCP client under Enterprise Edge, you do not have to let your workstations know that Enterprise Edge is your Internet gateway.

When Enterprise Edge receives DNS requests from clients, it first checks its local cache for name entries and records. If found locally, Enterprise Edge immediately responds to clients. Otherwise, Enterprise Edge creates a new DNS request to the remote Primary or Secondary DNS servers on behalf of the client. If the remote DNS server responds with the requested records, they are forwarded to clients and cached in Enterprise Edge.

Guidelines for Using Enterprise Edge DNS service

Consider the following guidelines when using DNS:

- If you enable the Enterprise Edge DNS service, make sure that you configure each workstation on the network to use Enterprise Edge as DNS server.
- When you disable Enterprise Edge DNS service, set the DNS Server field in DHCP configuration to the remote DNS server IP address. If DHCP service is also disabled in Enterprise Edge, you must configure each workstation on your network to use the remote DNS server

1. To configure DNS services settings, select **Services**, and click on the **DNS** heading in the navigation tree.
   The DNS Summary screen appears.

2. Configure the DNS Summary attributes as per the table below:

Attribute	Description
Description	Allows you to view the description of the server in cache mode.
Version	Allows you to view the version of the software interface.
Status	Allows you to enable or disable the DNS cache proxy in Enterprise Edge.
Domain	Allows you to specify the domain name that Enterprise Edge and its DHCP clients uses. When you modify the Domain, the setting automatically copies to **Domain Name** global options under **DHCP** service.
Primary (and Secondary) Server	Allows you to specify the primary server IP address in a valid dot format. You can specify more than one address if you separate them by a space. DNS cache uses them in the order you specify, to resolve names.
Forward Timeout	Allows you to specify the time-out, in seconds, to resolve queries using the DNS servers that you specify in DNS server.

3. Press the **Tab** key to save the settings.

Note: The DNS proxy carries security features because it keeps all of the internal IP addresses from external web servers. For information on other security features, see NAT (Network Address Translation) on page 232 and IP Firewall Filters on page 235.

IP Routing

The **IP Routing** service setting allows you to select, add or delete routing protocol on specific interfaces, choose routing protocol options, and add or delete static routes.

Enterprise Edge supports the following IP routing protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Routing Information Protocol (RIP)

Enterprise Edge supports RIP, a widely-used protocol for managing routing information in a self-contained network, such as a corporate intranet. RIP measures the shortest path between two points on a network in terms of the number of hops between those points.

Enterprise Edge router sends RIP routing information updates that list all the other hosts it knows about, to its nearest neighbor host every 30 seconds. The neighbor host sends the information to its next neighbor, until all the hosts in the network know the routing paths, a state known as network convergence. RIP uses a hop count to determine network distance. Each router in the network uses the routing table information to determine the next host for the packet, until it reaches the destination.

Enterprise Edge supports on demand routing table update and periodic routing table update. On demand routing table update is available only on demand-dial interfaces. Periodic update operates efficiently on persistent links

For information on how to select RIP as your routing protocol, see Configuring IP Routing on page 201.

Open Shortest Path First (OSPF)

Open Shortest Path First protocol bases its path descriptions on “link states” that take into account additional network information. OSPF also lets the user assign cost metrics to a given host router so that some paths are given preference. OSPF supports a variable network subnet mask so that a network can be subdivided into areas. For information on how to select OSPF as your routing protocol, see Configuring IP Routing on page 201.

WARNING

Because OSPF is a “link-state” based routing protocol, you must not use OSPF on demand dial interfaces. Frequent link status (between “up” and “down”) may cause the protocol to become unstable.

Configuring IP Routing

The followings table shows the Enterprise Edge IP routing protocols and the precedence order when conflicting or redundant routes occur.

Precedence	IP Routing Protocols
1.	Static Routing
2.	OSPF
3.	RIP v1 and v2

IP Routing global settings

To configure global settings for IP Routing:

1. Choose **Services** and click the **IP Routing** heading.
   The IP routing Summary, RIP Global Settings and OSPF Global Settings configuration screens appear.

2. Configure the Routing Summary attributes according to the following table:

Attribute	Description
Description	Shows a description of the router.
Version	Shows the version of the router.
Status	Allows you to enable or disable the router. The possible values are: **Up**: the IP router is currently functioning. **Enabled**: allows you to enable the router. **Disabled**: allows you to disable the router.

3. If your network uses RIP, configure the RIP Global Settings according to the table below. If your network uses OSPF, go to step 6.
   The RIP Global Settings are:

RIP Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
Triggered Update Interval	Allows you to specify the minimum interval, in seconds, at which a router must send a routing table update if the metric for a given route changes. If the router detects a change in the routing information, the router sends an update message at the specified interval. Possible values are **1** to **50000**. The default value is **5.**

4. Press the **TAB** key to save your settings.

   Note: After you configured global settings, you must configure each interface to use the IP routing protocol of your choice. For more information, see Configuring IP routing on an interface on page 202.

5. If OSPF is the routing protocol of your choice, configure the OSPF Global Settings according to the following table:

Attribute	Description
OSPF Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
Router ID	Allows you to specify the IP address that uniquely identifies the Enterprise Edge router on your network.
Router Area ID	Allows you to specify the area where your Enterprise Edge router is located on your network. The default value is **0.0.0.0**.
Authentication Type	Allows you to enable or disable password authentication. Values are **None**, **Password**. The default value is **None**. Note: For information on how to set the authentication password, see Configuring OSPF Parameters on a network interface on page 205.

Configuring IP routing on an interface

After you configured the IP Routing global settings, you must configure each available network interface to use the routing protocol of your choice or static routes..

Tips

You must use the same routing protocol on all interfaces. For example, you can not configure your LAN1 interface to use RIP, and your WAN1 interface to use OSPF.

This section provides instructions on how to configure interfaces for IP routing and how to create static routes. The available interfaces appear under the **IP Routing** heading. Follow the same instructions to configure all interfaces. For information on how to create static routes, see Static routes on page 207.

Configuring RIP parameters on a network interface

1. Under the **Services** heading, click the **IP Routing** key to expand the navigation tree.
   The available interfaces for IP routing are listed under the **IP Routing** heading.

2. Click the interface you want to configure.
   The Summary window appears. The **Routing Protocol** box shows the current routing protocol.

Tips
If you are changing the routing protocol from OSPF to RIP, you must first set the **Routing Protocol** under each available interface to **None** before you can select **RIP**.

Note: The RIP Parameters window does not appear unless you choose RIP as your routing protocol.

3. In the **Routing Protocol** list, choose **RIP**.

4. Press the **Tab** key.
   The RIP Parameters window appears.
   Configure RIP Parameters screen according to the following table:

Attribute	Description
Metric	Allows you to assign a cumulative value (in terms of hop count or associated cost [if applicable]) to routes passing through this interface. The routing manager adds the metric value of all routes learned through this interface to the metric value of this interface to make routing decisions. The possible values are **1** to **16**. Because RIP protocol can handle up to 15 hop counts before reaching destination, a value of **16** corresponds to "counting to infinity" The default value is **1**.
Routing Table Update Mode	Allows you to specify the routing table update mode. The possible values are: **On Demand:** the router sends its table when another established router requests it. **Periodic**: the router sends its table to other established router at regular intervals. The default value is **Periodic.**

Attribute	Description
Route Announcement Type	Allows you to set the type of routing table update announcements the Enterprise Edge router sends to other routers. The possible values are: **Disabled**: disables sending RIP routing update. If you choose **Disabled**, you must configure the other routers in the subnet to use static routes to access the Enterprise Edge server. **RIP 1**: sends only announcements of RIP v1 type in broadcast mode. **RIP 1 Compatible**: sends RIP v1 and RIP v2 packets in broadcast mode. Use this for a network environment which uses RIP v1 and RIP v2. **RIP 2**: sends RIP v2 packets in multicast mode only. Use this type of announcement only if all other routers connected to the Enterprise Edge server support RIP v2. The default value is **RIP 1**.
Route Accept Type	Allows you to set the type of routing table update announcements the Enterprise Edge router accepts from other routers. The possible values are: **Disabled**: disables sending RIP routing table update announcements. If you choose **Disabled**, you must create static routes in the Enterprise Edge server to access other networks connected to this interface. This method is preferable if you want to keep the routing table small in the Enterprise Edge server. **RIP 1**: accepts only announcements of RIP **1** type. **RIP 1 Compatible**: accepts announcements of RIP 1 and RIP 2 types. **RIP 2**: accepts announcements of RIP 2 type only.
Route Expiration Interval	Allows you to define the period of time within which a route in the routing table must be updated to remain a valid route. The possible values are **15** to **259200** seconds**.** The default value is **180** seconds.
Route Removal Interval	Allows you to define the period of time (in seconds) an invalid route remains in the routing table before the routing manager removes it from the routing table. The possible values are **15** to **29200** seconds**.** The default value is **180** seconds
Route Announcement Interval	Allows you to set the time interval (in seconds) between each routing table updates when the **Routing Table Update Mode** is set to **Periodic**. The possible values are **5** to **84200**. The default value is **30** seconds.
Route Tag	Allows you to create a special tag which identifies routes announced over the interface. The route tag helps identify route packets when debugging routing problems using a network sniffer.

Attribute	Description
Poisoned Reverse	Allows you to enable or disable options designed to avoid routing problems such as loops or metric values exceeding the maximum of 15 hop counts the RIP protocol allows. The following options are available: **Actual**: routing table update process where a routing table update going out repeats the information sent by the originator. The system tries to solve this state known as a loop involving two routers by sending more routing updates. **Split** (split horizon): routing table update process designed to avoid sending the same routing information back to the originator. **Poison Reverse**: routing table update process designed to advertise unreachable routes as having metric value of 16 regardless of incoming routing update information. The default value is **Split**.
Triggered Updates	Allows you enable immediate route update announcements whenever a metric or other information changes in the route table entries. When **Triggered Updates** is set to **Enabled**, the system gathers new routing information for the period of time defined in the **Triggered Update Interval** from the RIP Summary window (see IP Routing global settings on page 201). Triggered updates results in more frequent, smaller RIP routing table updates. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.
Announce Default Route	Allows you to enable or disable the announcement of default routes in incoming route announcements. Use caution when you enable this feature because improper configuration causes a loss of network connectivity. The possible values are **Enabled** and **Disabled**. The default value is **Disabled**.
Accept Default Route	Allows you to enable or disable the acceptance of incoming default routes announcement. Set default routes as static routes. If you run Net Link Manager to automatically backup primary WAN link using a dial-up link, Net Link Manager manages the default routes and the default routes that you add are non-operational as soon as a primary link breaks or comes up again. The possible values are **Enabled** and **Disabled**. The default value is **Enabled**.

5. Press **Tab** to save your settings.

Configuring OSPF Parameters on a network interface

1. Under the **Services** heading, click the **IP Routing** key to expand the navigation tree.
   The available interfaces for IP routing are listed under the **IP Routing** heading.

2. Click the interface you want to configure.
   The Summary window appears. The **Routing Protocol** box shows the current routing protocol.

Tips

If you are changing the routing protocol from RIP to OSPF, you must first set the **Routing Protocol** under each available interface to **None** before you can select **OSPF**.

Note: The OSPF Parameters window does not appear unless you choose OSPF as your routing protocol.

3. In the **Routing Protocol** list, choose **OSPF**.

WARNING

Because OSPF is a "link-state" based routing protocol, you must not use OSPF on demand dial interfaces. Frequent link status changes (between "up" and "down") may cause the OSPF protocol to become unstable.

4. Configure the OSPF parameters according to the following table:

Attribute	Description
Metric	Allows you to assign a cumulative value (in terms of hop count or associated cost [if applicable]) to routes passing through this interface. The routing manager adds the metric value of all routes learned through this interface to the metric value of this interface to make routing decisions. The possible values are **1** to **16**. Because RIP protocol can handle up to 15 hop counts before reaching destination, a value of **16** is equal to "counting to infinity" The default value is **2**.
Interface Type	Allows you to select the type of interface that describes your network configuration. The possible values are: **Broadcast** a broadcast network supports multiple routers and addresses a single physical message to all routers. **P2P** a point-to-point network joins a single pair of OSPF routers. **NBMA** a Non-Broadcast-Multi-Access (NBMA) network supports multiple routers and cannot address a single physical message to all routers. The default value is **Broadcast**
Router Priority	Allows to assign a priority to the Enterprise Edge router. The possible values are **0** to **255**. A value of 0 indicates that the Enterprise Edge system cannot become the designed router. The default value is **1**.
Transit Delay	Allows you to set (in seconds) the estimated round-trip transit delay in the network connected to the interface. The values are **1** to **3600** seconds. The default value is **1**.
Retransmit Delay	Allows you to set the number of seconds the router waits before retransmitting after a time-out occurs. The values are **1** to **3600** seconds. The default value is **1**.
Hello Interval	Allows you to define how frequently the router must send "hello packets" on an interface. The values are **1** to **32767** seconds. The default value is **10**.

Attribute	Description
Dead Interval	Allows you to set the maximum number of seconds the router waits to receive the next hello before considering the adjacent router as non operational. The values are **1** to **32767** seconds. The default value is **40.**
Poll Interval	Allows you to define the period of time the router must keep sending hello packets to an adjacent routing which is considered non operational. The values are **1** to **32767** seconds. The default value is **120**
MTU	Allows you to specify the Maximum Transmission Unit for this interface. The values are **1** to **10000**. The default value is **1500**
Password	Allows you to define an authentication password (if you selected **Password** as the authentication type in the **Authentication Type** box on the OSPF Global Parameters window. There is no default value provided because the **Authentication Type** is set to **None** by default.

5. Press the **Tab** key to save your settings.

Static routes

You can add static routes to the Enterprise Edge routing table. Static routes on added to the routing table take precedence over dynamic routes. To add a static route to the routing table:

1. Under the IP Routing heading, click on the interface for which you want to create a static route.
   The **Configuration** menu is enabled.

2. On the **Configuration** menu, click **Add Static Route**.
   The Static Route dialog box appears.

3. Configure the static route attributes according to the following table:

Attribute	Description
Static Route (SR#)	Allows you to assign a number to the static route. For example, the valid static route number for the first static route is SR1. If you add more than one static route, use sequential numbers. If you use the number of an existing static route, the system modifies the existing static route. If you use non-sequential numbers the system automatically reassigns sequential numbers. When you modify a static route, you cannot change the number. The only function of the static route number is to uniquely identify an route.
Destination address	Allows you to define the IP address of the destination network or host.
Destination mask	Allows you to add the IP address of the mask corresponding to the destination address.
Next Hop Router	Allows you to define the IP address of next hop router.

Attribute	Description
Metric Value	Lets you specify the metric value associated with the interface. The system adds the metric to the hop count of the routes received through the interface.

4. Click save.
   The static route is added to the list in the Static Route window.

To modify the configuration of a static route:

1. Click a static route you want to modify in the **Static Route** table.
   The Static Route row is highlighted.

2. On the menu, click **Configuration** and then click **Modify Static Route**.
   The Static Route dialog box appears.

3. Modify the static route attributes.

4. Click the **Save** button.

To delete a static route:

1. Click the static route you want to delete in the **Static Route** table.

2. On the menu, click **Configuration** and then click **Delete Static Route**.

3. A message ask you to confirm your request

4. Click the Yes button.

IPX Routing

Enterprise Edge supports RIP and SAP (Service Advertising Protocol) for IPX routing in a NetWare environment. Static routes and static services are also supported.

Enterprise Edge supports IPX basic packet filtering feature.

Configuring IPX Routing

1. Choose **Services**, and click on the **IPX Routing** heading.
   The Global Parameters for IPX Router appears.

2. Use the following table to configure the IPX global settings.
   The Summary, IPX Global Summary, RIP Global Settings and SAP Global settings are:

Attribute	Description
Description	Displays the name of the router.
Version	Displays the version number of the router.
Status	Displays the current status of the service. Possible values are **Disabled**, **Up**, **Down**. Users can change the status of the service by selecting **Disabled** or **Enabled**. By default, IPX service is **Disabled**.
Internal Network Number	Allows you to specify the internal network number. The internal network number uniquely identifies the computer on the intranet.
IPX Log level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
RIP Log level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.
SAP Log Level	Allows you to enable the recording of events in the Event Viewer. The following options are available: **Maximum**, logs all information in the Event Viewer. **Warnings Also**, logs errors and warnings in the Event Viewer. **Errors Only,** logs errors in the Event Viewer. **Disabled,** disables event logs. The default value is **Errors Only**.

3. Press the **Tab** key to save the settings.

Configuring an interface for IPX routing

This section provides instructions on how to configure IPX routing for specific interfaces. All available interfaces (i.e.: LAN2, WAN1, V90-1) appear under the IPX Routing heading. The same configuration procedures apply to all interfaces.

1. Choose **Services**, and click on the **LAN1** heading (if configuring IPX routing for traffic on LAN1).
   The IPX routing parameters for LAN1 appear.

2. Configure LAN1 for IPX routing using the following tables.
   The Interface Summary settings are:

Attribute	Description
Interface Name	Displays the name of the interface you are currently configuring for IPX routing.
Input Filter Actions	Allows you to specify the action the filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for filters. **Permit** all inbound traffic matching the criterion defined for filters. The default value is **Deny**. Note: You must create a filter before you can assign an action. To create a filter, see Adding RIP filters for IPX routing on page 213.
Output Filter Actions	Allows you to specify the action the filter must perform on outbound traffic. The values possible values are: **Deny** all outbound traffic matching the criterion defined for filters. **Permit** all outbound traffic matching the criterion defined for filters. The default value is **Deny**. Note: You must create a filter before you can assign an action. To create a filter, see Adding RIP filters for IPX routing on page 213.
Network Number	Allows you to specify the network number (also called external network number) for routing purposes.
Frame Type	Allows you to specify the frame type. For example, an Ethernet 802.2 frame type value is **2ff**. Ethernet II: **0**, Ethernet 803.2: **1**, Ethernet 802.2: **2**, SNAP: **3** Arcnet: **4**. System default shows only the suffix **ff**.

The RIP Parameters settings are:

Attribute	Description
RIP State	Allows you to enable or disable RIP for this interface. The values are **Enabled** or **Disabled**.
Advertise Routes	Allows you enable or disable the advertisement of routes on the interface your configuring. The default value is **Disabled.**
Accept Route Advertisements	Allows you to enable or disable the acceptance of route advertisement from remote routers on this interface. The default value is **Enabled.**
Update Mode	Allows you to select an update mode for the routing table. The routing table update modes available are: **Standard** update mode sends out a router's routing table at regular intervals (which you specify in the Update Interval box). New routes are added to the routing table as dynamic routes and are deleted from the routing tables when the router restarts. **Autostatic** update mode sends a routing table on the current interface when other routers connected to this interface request it. New routes to this interface, using RIP, are stored as static routes in the routing table for this interface and remain until you delete them. **No Update** mode never updates the routing tables on the current interface.

Attribute	Description
Update Interval	Allows you to set at what interval (in seconds) the routing manager updates the route tables. For example, when you set the Update Mode to **Standard,** the routing manager periodically updates the route tables at the interval you specify in the Update Interval box. The possible values are 5 to 86400 seconds (24 hours) Default value is 60 seconds.
Aging Interval Multiplier	A multiplier used to determine when a route expires and is removed for the route table. For example, if the update interval is set to 60 seconds and you enter a value of 3 in the Aging Interval Multiplier, a route remains in the route table for a maximum of 180 seconds (3 X 60) from the last update. The default value is 3.

The RIP Input/Output Filters settings display the filter number, Network number and Network Mask. To add an input or output RIP filter refer to Adding RIP filters for IPX routing on page 213.

The SAP Summary settings are:

Attribute	Description
Input Filter Actions	Allows you to specify the action the filter must perform on inbound traffic. The values possible values are: **Deny** all inbound traffic matching the criterion defined for SAP filters. **Permit** all inbound traffic matching the criterion defined for SAP filters. The default value is **Deny**. Note: You must create a filter before you can assign an action. To create a filter, see Adding SAP filters for IPX routing on page 214.
Output Filter Actions	Allows you to specify the action the filter must perform on outbound traffic. The possible values are: **Deny** all outbound traffic matching the criterion defined for SAP filters. **Permit** all outbound traffic matching the criterion defined for SAP filters. The default value is **Deny**. Note: You must create a filter before you can assign an action. To create a filter, see Adding SAP filters for IPX routing on page 214.

The SAP Parameters settings are:

Attribute	Description
SAP State	Allows you to enable or disable SAP for this interface. The values are **Enabled** or **Disabled**.
Advertise Services	Allows you to enable or disable the advertisement or SAP services on the interface to remote routers. Possible values are **Enabled** or **Disabled**. The default value is **Enabled**.
Accept Service Advertisements	Allows you to enable or disable the acceptance of advertisement of SAP services from remote routers. Possible values are **Enabled** or **Disabled**. The default value is **Enabled.**
Update Mode	Allows you to select an update mode for SAP on the interface. The available options are: **Standard** update mode sends periodic updates at interval you define in the Update Interval box. **Autostatic** update mode sends a routing table update when other routers connected to this interface request it. New routes to this interface, using SAP, are stored as static routes in the routing table for this interface and remain until you delete them. **No Update** mode never updates the routing tables on the current interface. If you are configuring IPX routing on a LAN interface, the default value is **Standard**. If you are configuring IPX routing for a WAN interface, the default value is **No Update**.
Update Interval	Allows you to set the interval (in seconds) at which SAP announcements are updated. For example, if you set the **Update Mode** to **Standard**, the SAP announcements are updated at the interval you specify in the Update Interval box. The possible values **5** to **86400** seconds. The default value is **60** seconds.
Aging Interval Multiplier	A multiplier used to determine when a SAP announcements coming to this interface expire. For example, if the update interval is set to 60 seconds and you enter a value of 3 in the Aging Interval Multiplier, a SAP announcement remains valid for a maximum of 180 seconds (3 X 60) from the last announcement. The possible values are **3** to **100**. The default value is **3**.

The SAP Input/Output Filters settings display the Service Type, Service Name and Network Mask. To add an input or output SAP Filter refer to Adding SAP filters for IPX routing on page 214.

The Static Routes settings display the Static Route number, Net Number, Next Hop Mac Address, Ticks and Hops. To add a Static Routes refer to Adding Static Routes for IPX Routing on page 214.

The Static Service settings display the Static Service number, Type, Name, Network, Node, Socket and Hops. To add a Static Service refer to Adding Static Service for IPX on page 215.

Adding RIP filters for IPX routing

RIP is the routing protocol that routes IPX data packets in an internetwork environment. IPX Router Manager (Windows NT 4.0 routing management entity) is responsible for IPX routing operation. You can configure IPX packet filters for inbound or outbound traffic on interface handling IPX packets. You must configure the IPX RIP parameters from the IPX heading of the navigation tree (Configuring IPX Routing on page 208).

Note: The IPX router manager in your Enterprise Edge system operates separately from the IP routing manager. As a result, RIP configuration under the IP Routing heading has no effect on IPX routing. You must configure IPX RIP parameters under the IPX Routing heading.

Tips

After you create and add a filter for IPX routing on an interface, you must select The Input Filter Action and Output filter Action from the RIP Summary parameters.

Warning

The filter action which indicates either to deny or allow packets that match filter definition applies to all filters. You cannot set a filter action for a specific filter. When you have decided which action the routing manager must perform on packets matching a filter definition, the routing manager performs this action every time it finds a match between packets and filters.

To add a RIP filter for IPX routing:

1. Choose **Services**, **IPX Routing** and click on the interface you want to configure.

2. On the **Configuration** menu click **Add RIP Input Filter** or **Add RIP Output Filter**.

3. Use the table below to set your RIP Input or Output filter parameters for IPX routing:

Attribute	Description
Input Filter (IF#)	Allows you to give a number to the input filter you are creating.
Output Filter (OF#)	Allows you to give a number to the output filter you are creating.
Network Number	Allows you to enter the network number that identifies the IPX network. A valid entry is any 4-byte hexadecimal number.
Network Mask	Allows you to enter the network mask to be applied to the source address. This parameter defines the range of network numbers that you want to filter.

4. Click **Save**.

Adding SAP filters for IPX routing

On a Novell network, the Service Advertising Protocol (SAP) provides network control information about available services on a Novell network. You can define and add SAP filters for IPX routing.

1. Choose **Services**, **IPX Routing** and click on the interface that you want to configure.
2. On the **Configuration** menu click **Add SAP Input Filter** or **Add SAP Output Filter**.
3. Use the table below to set your SAP Input or Output filter parameters for IPX routing:

Attribute	Description
Input Filter (SapIF#)	Allows you to give a number to the input filter you are creating.
Output Filter (SapOF#)	Allows you to give a number to the output filter you are creating.
Service Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Service Name	Allows you to enter the service name. You can use a wildcard service name such as "*" to indicate all service names.

4. Click **Save**.

Adding Static Routes for IPX Routing

You can add static routes to the IPX routing table. The IPX static routes take precedence over the routes added by routing protocol such as RIP.

1. Click on the **IPX Routing** key to expand the heading.
2. Click on the LAN or WAN interface that you want to configure. For example, **LAN1**.
3. Under the Configure menu choose Add Static Route.
   The Static Routes dialog box appears.
4. Configure the LAN1 (and WAN1, WAN2, etc.) static routing table attributes according to the table below.

The following table shows parameters required for IPX static routes:

Attribute	Description
Static Route (SR#)	Enter a Static Route number.
Net Number	IPX Network Number identifies the destination network for the routing table entry. The permitted value is 4-byte in hexadecimal format. The default value is **None**
Next Hop MAC Address	Shows the MAC address of the next hop router to reach the network defined in the **NetNumber** box. The permitted value is 6-byte in hexadecimal format. The default value is **None**.
Ticks	Time required (in 1/60 seconds) to reach the destination network. The values are **1** to **32,767**. The default value is **None**.
Hops	Shows the number of hops that must be crossed in order to reach the destination network. The permitted values are **1** to **15**. The default value is **None**.

Adding Static Service for IPX

1. Click on the **IPX Routing** key to expand the heading.

2. Click on the interface that you want to configure. For example, **LAN1**.

3. Under the Configure menu choose **Add Static Service**.
   The Static Routes dialog box appears.

4. Configure the LAN1 (and WAN1, WAN2, etc.) static service table attributes according to the table below:
   The attributes for adding Static services in the IPX network are:

Attribute	Description
Static Service	Show the service type (SS Number). The permitted value is in 2-byte hexadecimal format. The default value is **None**.
Type	Allows you to specify the SAP service type. Use a 2 byte hexadecimal number. You can use the value 0xFFFF to match services of any type.
Name	Shows the static service name. The permitted values can use up to 48 bytes. A wildcard character (*) can also be selected to indicate all service names.
Network	Shows the network part of the service address. The permitted value uses 4 bytes in hexadecimal format. The default value is **None**.
Node	Shows the node part of the service address. The permitted value uses 6 bytes in hexadecimal format. The default value is **None**.
Socket	Shows the socket part of the service address. The permitted value uses 2 bytes in hexadecimal format. The default value is **None**.
Hops	Shows the number of hops to reach the destination network. The permitted values are **1** to **15**. The default is **None**.

5. Click the **Save** button to save your settings.

SNMP

Enterprise Edge generates SNMP traps corresponding to events and reports those events to requesting management stations.

Guidelines for using SNMP

Consider the following guidelines when using SNMP:

- You can set read-only and read-write community names.
- You can set a list of permitted managers. When set, the agent responds to SNMP managers requests from those IP hosts only.
- An empty list of permitted managers implies that agent responds to requests from anyone.
- You can set trap communities. Each trap entry identifies the community name that must be used and the manager addresses.
- You can enable or disable sending authentication traps.
- You can enable or disable the SNMP agent.
- At present, SNMP supports only MIB-II (RFC 1213) MIBs.

1. Choose **Services**, and click on the **SNMP** heading.
   The screen displays the SNMP Summary, Community List, Manager List, and Trap Community List screens.

2. Configure SNMP summary screen from Unified Manager.
   Configure the SNMP Community List, Manager List, and Trap Community List from the menu.

The SNMP Summary attributes are:

Attribute	Description
Description	Shows the description of the SNMP agent.
Version	Shows the version of the SNMP agent
Status	Allows you to enable or disable the SNMP agent.
Authentication Failure Traps	Allows you to disable authentication failure traps. When enabled, the SNMP agent sends authentication failure traps if there is an authentication failure. Authentication failure happens if an SNMP manager application provides a wrong community string or performs an operation that is not permitted for a community.

To modify the SNMP Summary attributes:

1. From the **Status** list, select **Enabled**, **Disabled** or **Up**.

2. From the **Authentication Failure Traps** list, select **Enabled** or **Disabled**.

3. Press the **Tab** key to save the changes.

SNMP Community List, Manager List, and Trap Community List

The SNMP community list, manager list, and trap community list attributes are:

Attribute	Description
Community List	Allows you to specify the entry name used as a key to uniquely identify an individual community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix C followed by a unique number that identifies the community name entry on the agent. For example, C2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing community entry name, it modifies the existing community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a community entry, you can't change the name. The community entry name does not have any significance other than to identify an entry.
Community Name	Allows you to specify the name of the community that the individual managers use to interact with this agent. When creating community entries, various access permissions are associated with these names. Manager stations that use different community names get different permissions on the SNMP agent. While creating trap communities, various manager IP addresses are associated with these values. All the manager stations in a trap community get traps with the community name specified in the entry.
Manager List	Allows you to specify the entry name used to identify an individual manager entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix M followed by a unique number that identifies the manager entry on the agent. For example, M2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing manager entry name, it modifies the existing manager entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a manager entry, you can't change the name. The manager entry name does not have any significance, other than to uniquely identify an entry.
Manager IP address	Allows you to specify the IP Address of the SNMP Manager station corresponding to this entry. If no manager entries are created, the Enterprise Edge device accepts SNMP requests from all stations. If there is a list of manager entries, Enterprise Edge server accepts SNMP requests from the IP Addresses specified in the list.
Trap List	Allows you to specify the entry name used to identify an individual trap community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix T followed by a unique number that identifies the trap community entry on the agent. For example, T2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing trap community entry name, it modifies the existing trap community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a trap community entry, you can't change the name. The trap community entry name does not have any significance, other than to uniquely identify an entry.

To modify the Community List, Manager List, and Trap Community List, use the following procedures.

To add to the community list:

1. On the **Configuration** menu, click **Add Community**.
   The Community List dialog box appears.

2. Click the **Community List** box and type the community list number.

3. Click the **Community Name** box and type the community name.

4. From the **Access Permission** list, select the Access Permission.

5. Click the **Save** button.

To modify a community:

1. Click a community in the **Community** table.

2. On the **Configuration** menu, click **Modify Community**. The Community List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button.

To delete a community:

1. Click on a community in the **Community** table.

2. On the **Configuration** menu, click **Delete Community**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion.

To add a manager to the Manager List:

1. On the **Configuration** menu, click **Add Manager**.
   The Manager List dialog box appears.

2. In the **Manager List** box, type the manager list number.

3. In the **Manager IP Address** box, type the manager IP address.

4. Click the **Save** button.

To modify the manager list:

1. In the **Manager List** table, click a manager.

2. On the menu, click **Configuration** and then click **Modify Manager**.
   The Manager List dialog screen appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button.

To delete a manager:

1. In the **Manager** table, click the manager you want to delete.

2. On the **Configuration** menu, click **Delete Manager**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion.

To add a trap community to the Trap Community List:

1. On the **Configuration** menu, click **Add Trap Community**.
   The Trap Community List screen appears.

2. In the **Trap List** box, type the trap list number.

3. In the **Community Name** box, type the community name.

4. In the Manager IP Address box, type an IP Address for a manager station that is a member of this trap community.

5. Click the **Save** button.

To modify a trap community:

1. In the **Trap Community** table, click the trap community you want to modify.

2. On the **Configuration** menu, click **Modify Trap Community**.
   The Trap Community List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button.

To delete a trap community:

1. In the **Trap Community** table, click the trap community you want to delete.

2. On **Configuration** menu, click **Delete Trap Community**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion.

QoS

The purpose of the Enterprise Edge QoS module is to set priorities for IP traffic and to assign quality of service levels to critical applications and IP telephony.

The Enterprise Edge QoS module serves two primary purposes:

- In a DiffServ network, QoS acts as an edge device and performs the packet classification, marking, and prioritizing.
- In a non-DiffServ or legacy network, QoS manages the WAN link bandwidth to make sure critical voice (and optional video) packets get high priority when crossing the slow WAN link in both directions.

Relationship between the QoS Module and the VoIP QoS Monitor

The VoIP gateway in Enterprise Edge includes a VoIP Quality-of-Service (QoS) Monitor that periodically monitors the delay and jitter of IP networks between two peer gateways by using a proprietary protocol. These monitoring packets are delivered at UDP port 5000.

The main objective of the VoIP QoS Monitor is to allow new VoIP calls to fall back to the PSTN if the IP network is detected as “bad”.

The QoS module discussed here complements the VoIP QoS Monitor. While the VoIP QoS Monitor passively monitors the IP network, the QoS module actively improves the IP network by giving VoIP packets higher priority to travel so that the chance for the VoIP QoS Monitor to detect the connection as “bad” is reduced.

Note: For a VoIP call, if a packet passes the VoIP QoS Monitor but fails the QoS admission control, it is delivered over IP but only as a best-effort flow. There is no fallback to PSTN if a packet has passed the VoIP QoS Monitor checking.

VoIP QoS Monitor packets travel at the same priority as VoIP packets, which is at higher priority than normal IP packets. If VoIP packets travel at a premium level but VoIP QoS Monitor packets travel at normal best-effort level, it is possible for the VoIP QoS Monitor to report the IP network as “bad” and start fallback to the PSTN, but the actual delay and jitter for VoIP packets are still “good” since VoIP packets have a higher priority. To avoid this, add UDP port 5000 to the high priority queue in all routers.

QoS Restrictions and Defaults

Enterprise Edge QoS includes the following restrictions and defaults:

- By default, the general bulk of traffic (not defined by priority filters) is routed to best-effort Queue 5 (with Queue 1 the highest priority and Queue 8 the lowest). An administrator can define four classes of traffic above the generic traffic and three classes below it.
- A maximum of 31 priority filters for best-effort traffic can be created.
- The QoS module can be Enabled or Disabled. The default setting is Enabled.
- The predetermined WAN bandwidth is always available to VoIP gateway channels. That is, VoIP gateway calls are always admitted. The remaining WAN premium bandwidth can be used by other H.323 streams, such as Microsoft NetMeeting. If there is no VoIP gateway traffic, the VoIP WAN bandwidth can be used only by best-effort traffic, not other premium traffic (for example, NetMeeting). Enterprise Edge does not support preemption of admitted premium streams.
- Currently, packet prioritizing and priority filters apply only to outbound traffic for specified interfaces. Inbound traffic is treated on a first in/first out (FIFO) priority.
- The maximum port numbers you can reserve for premium traffic is 256.

To configure QoS services settings:

1. Choose **Services** and click on the **QoS** heading.
   The QoS Summary screen appears.

2. Configure the QoS Services Summary attributes according to the following table:

Attribute	Description
Description	Shows the description of the QoS provider.
Version	Shows the driver version of the QoS provider.
Status	Allows you to enable or disable the QoS module.

Attribute	Description
Premium Bandwidth	Allows you to specify, in percentages, the WAN bandwidth reserved for premium traffic. Choose a value for this box based on the link speed, the codecs used by VoIP gateway, the sample rate and the number of concurrent phone calls (from internal VoIP gateway) and other H.323 sessions (like Microsoft NetMeeting traffic) you intend to carry over the WAN link. Refer to WAN Overview on page 49 for more information on this topic. Make sure you allocate at least the bandwidth necessary to carry as many phone calls as specified in 'Number of Phone Ports' box below. Otherwise, the QoS provider sees the inconsistent configuration and disables itself when system boots next time, resulting in broken connectivity. Any additional bandwidth that is more than what is required to carry the phone calls is available for other H.323 sessions, like NetMeeting sessions from PCs connected to Enterprise Edge box or other data traffic classified as premium, through QoS Filters. This additional bandwidth reserved for premium traffic is always available for other data traffic if there is no additional H.323 traffic or other premium traffic. A network administrator can reserve more WAN bandwidth than that required to carry phone calls and then prevent PC users from using it for NetMeeting sessions by setting filters that drop H.323 traffic at LAN interfaces.
Video Class	Allows you to specify the type of priority treatment for video traffic in H.323 sessions. The following choices are available: **Premium**: Video traffic is treated as premium traffic that consumes portions of bandwidth reserved for premium traffic (Premium Bandwidth box). **Best Effort**: Video traffic is treated as best effort IP traffic that are prioritized among other best-effort traffic passing through the WAN link.
Premium DS Code	Allows you to specify the TOS setting in the IP header for premium packets. This value is used in conjunction with the frame relay driver in Enterprise Edge's WAN link, if one is being used, as well as rest of the network. If the frame relay is used on WAN link, this code should match the DS Code setting in frame relay settings so that frame relay network treats this traffic as high-priority. If rest of the network is diffserv capable, all routers that carry VoIP traffic from theEnterprise Edge server must be configured to treat the traffic with this DS code as high-priority or premium traffic.
Number of Phone Ports	Allows you to specify the number of phone ports. This value specifies the number of concurrent phone calls user intends to carry over the WAN interface. QoS Provider layer uses this value to determine how much of the bandwidth reserved for premium traffic is consumed by internal VoIP gateway and how much is left over for other H.323 or other classified premium traffic.

3. Press the **Tab** key to save the settings.

Filters

The Filters heading allows you to configure different Filters for QoS and specify the order that these filters are evaluated. Configure the filters before you specify the filter order. If a filter name is listed in filter order, but the actual filter is missing, the system ignores it. If a filter is omitted from the filter order list, the filter is not effective.

To set QoS filters:

1. Choose **Services**, **QoS** and click on the **Filters** heading.
   The Filter Configuration and Filters screen appears.

Adding a QoS filter

2. On the **Configuration** menu click **Add Filters**.
   The **Filters** property sheet appears.

3. Set the QoS Filters parameters according to the following table:

Attribute	Description
Filter	Allows you to specify the entry name that is used as a key to uniquely identify an individual filter entry in QoS layer. Its value must follow certain conventions. It must have the prefix F followed by a unique number that identifies this filter. For example, F2 is a valid value. While adding, specify non-recurring values for the unique number. If you specify an existing filter entry name, the system modifies the existing filter entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter entry, you can't change the name.
Source Address	Allows you to specify the source IP address in a valid dot format. If you want to ignore the source address setting in filter, leave this box blank. If you specify an address in this box, you should also specify a subnet mask in the Source Mask box.
Source Mask	Allows you to specify the source mask of the IP address in a valid dot format. If you specify a source address, you must specify a source mask and vice versa. Make sure that the mask and address match with each other, for example bitwise and of mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, address/mask combination 10.10.10.32/ 255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.
Destination Address	Allows you to specify a destination IP address in a valid dot format. See the instructions for Source Address.
Destination Mask	Allows you to specify a mask for the destination IP address in a valid dot format. See the instructions for Source Mask.

Attribute	Description
Source Port	Allows you to specify a source port to match the filter. Specify a source port only if you choose a TCP or a UDP protocol. If you do not want to include the source port in your filter, select IGNORE for it. Otherwise, select the port for one of the well-known services from the list or type it in the list. If you type the port, specify the service's numeric port number. You can specify a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can also specify 0 for the lower limit and 65536 for upper limit.
Destination Port	Allows you to specify a destination port to match the filter. It is interpreted the same way as source port.
Protocol	Allows you to specify a protocol to match the filter. If you do not want to include a protocol in your filter, select IGNORE for the protocol. Otherwise, select the protocol from the list or type the numeric value of sub-protocol under IP in the box.
DSCode (TOS) Criteria	Allows you to specify the DS Code (TOS) value for the filter to match. Use this setting only if your network or application behind Enterprise Edge is diffserv capable or diffserv aware. Specify here the DS Code or TOS value that the application or the other edge device puts in the IP packets it sends. Otherwise, ignore this setting.
Priority	Allows you to specify the priority given to packets that match the criteria specified in the filter. The priority value has significance only within the IP interface the packet is related, and is relative to other packets that go out through the interface. 0 is the highest priority and 8, the lowest priority. Use caution when you assign priority. If you assign priority 0 for regular data traffic, it is possible that the quality of voice calls that go through this interface are degraded. Use priority 0 only if your WAN does not carry any voice calls. As a guideline, always start assigning priorities from the lowest level up.
Outbound DS Code	Allows you to specify the new DS Code added to the packets that match this filter. If you do not want to change the DS Code in the packets going out through the interface, don't specify any value for this setting. If a value is specified, this setting lets Enterprise Edge change the DS code on outgoing packets. This lets Enterprise Edge be used as a 'marker' device on the edge of a diffserv capable network.

4. Click **Save**.

5. In the Filter Configuration screen specify the order of the Filters from the most important to the least important.

QoS performance graphs and tables

To access QoS performance graphs and tables:

1. Choose **QoS**, click **Performance** on the menu bar and then click **QoS Session Graph**.
   The QoS Performance Graph appears.

2. On the menu, click **Performance** and then click **QoS Session Table**.
   The QoS Performance Table appears.

3. Access the remaining QoS graphs and QoS tables by following the steps for QoS Session Graphs and Tables.

Port Range Setting for Legacy Networks

Enterprise Edge uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. You must reserve these same port ranges and set them to high priority on all routers that an administrator expects to have QoS support. You do not need to reserve port ranges on DiffServ networks.

You can select any port ranges that are not used by well-known protocols or applications.

Each H.323 or VoIP RTP flow uses two ports. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

- Backbone routers reserve more ports than edge routers.
- The port ranges on edge routers are a subset of the backbone router port ranges.
- Include port number UDP 5000 in the reserved port ranges.
- The port ranges reserved in an Enterprise Edge system are also reserved by the remote router.
- You must reserve two ports for each voice call you expect to carry over the WAN link. The system requires two additional ports for each video session if the video traffic is treated as premium traffic.
- You can reserve multiple discontinuous ranges. Enterprise Edge requires that each range meet the following conditions:

  - Each range must start with an even number.

  -There must be an even number of ports in a range.

See Appendix C: Setting Up Remote Routers on page 389 for additional information on setting UDP port ranges on remote routers.

To set the QoS port ranges:

1. Choose **QoS** and click on the **PortRanges** heading.
   The QoS PortRanges screen appears.

To modify port ranges:

1. In the **Port Ranges** table, click the port ranges you want to modify.

2. On **Configuration** menu, click **Modify Port Ranges**.
   The Port Ranges screen appears.

3. In the **Begin** box, type the beginning value for the range.
   This must be an even value.

4. In the **End** box, type the appropriate end value for the range.

5. Click the **Save** button.

To add port ranges:

1. On the **Configuration** menu, click **Add Port Ranges**.
   The Port Ranges dialog box appears.

2. In the **PortRange (R#)** box, type the port range number.
   Type an entry that looks like “Rxx” where “xx” is a unique number.

3. In the **Begin** box, type the beginning value for the range.
   This must be an even value.

4. In the **End** box, type the ending value for the range.

5. Click the **Save** button.

   Note: If the rest of your network is not diffserv capable, you can set filters in other routers to give higher priority to VoIP traffic. In all the routers that carry VoIP traffic from the Enterprise Edge server, you must set filters that classify the traffic to and from these port ranges as high priority.

To delete port ranges:

1. In the **PortRanges** table, click the port range you want to delete.

2. On the **Configuration** menu, click **Delete PortRanges**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm.

QoS monitor

To set the QoS monitor:

1. Choose **Services** and click on the **QoS Monitor** heading.
   The QoS Monitor Summary screen appears.

2. Configure the QoS Monitor Summary attributes according to the following table:

Attribute	Description
Description	Shows the description of the service monitor.
Status	Allows you to enable or disable the service monitor.
Version	Shows the version of the service monitor.

3. From the **Status** list, select **Enabled** or **Disabled**.

4. Press the **Tab** key to save the settings.

QoS Monitor Mean Opinion Score

To view the QoS Monitor Mean Opinion Score:

1. Choose **Qos Monitor** and click on the **Mean Opinion Score** heading.

   If you configure or create remote gateways by clicking the VoIP Gateway, Remote Gateway navigation key, the mean opinion scores of the connections to these remote gateways, which are a measure of quality of the voice link, while using IP trunk, for each codec type are displayed in the screen. Each configured gateway appears on a separate row.

   Each row consists of the fields for the name of the remote gateway, its IP address, the status of the QoS monitoring for the connection, and the mean opinion scores for each allowed voice codec types and for each direction.

   If the QoS Monitor setting for the remote gateway entry is Disabled the MOS value for the remote gateway is N/A. Also, if the QoS Monitor service is disabled or down for any reason, all MOS values are N/A.

   While MOS values are being shown, they are updated approximately every 50 seconds. To refresh the data, on the menu click **View** and then click **Refresh**.

2. Click the **QoS Monitor** navigation key to close the navigation tree.

Web cache

When you use Enterprise Edge as a web proxy, Enterprise Edge can store, or cache, information downloaded from the Internet. A proxy is a server that acts on behalf of another. Web caching allows LAN workstations to share common information downloaded from the Internet.

With Enterprise Edge configured as a web proxy with web caching:

- LAN workstations have shorter download times.
- The system stores previously downloaded information for future use by all workstations on the LAN.
- Enterprise Edge retrieves information from the Internet only if it is not already cached or if the cached file is out of date compared to the information on the Internet.

You can configure the web caching settings through your web browser.

The web proxy also provides security features similarly to the DNS proxy because it hides all of the internal browsers' IP addresses from external web servers. External web servers see only Enterprise Edge's IP address.

Guidelines for Using Web Caching/Proxy

The Enterprise Edge web proxy uses a web server for running in HTTP-Proxy mode.

Consider the following guidelines when using web caching/proxy:

- You cannot use a web server installed in Enterprise Edge as a general-purpose HTTP server. It is only used by the Enterprise Edge web-based management client and web-cache services.
- If users must run their web sites, they must run a separate HTTP server on a system different from Enterprise Edge and make its IP address known to the users of that site.

To configure the web cache settings:

1. On the navigation tree, choose **Services** and click on the **Web Cache** heading. The Web Cache Summary screen appears.

2. Configure the Web Cache attributes according to the table below:

Attribute	Description
Description	Shows the description of the Web Cache server.
Version	Shows the version of the Web Cache server.
Status	Shows the status of the Web Cache server. This setting is read-only. The server always runs to provide support for web-based UIs for Enterprise Edge.

Attribute	Description
Server Address	Allows you to tell the web server what IP address to use for interacting with HTTP clients. Since Enterprise Edge server typically has more than one IP interface and associated IP Address, users can choose this value. This value is automatically set to the IP Address of the first LAN interface and changes when the latter changes. Exercise caution if modifying this value.
Cache Mode	Allows you to enable or disable the cache-mode of operation.
Cache Size	Allows you to specify the maximum size (1 -1 100,000), in KB, of the cache.
Garbage Collection Interval	Allows you to specify the interval, in hours, between garbage collection operations on the cache. The values are **1** to **24**.
Cache Maximum Life	Allows you to specify the maximum life, in hours, on the proxy server for the HTTP pages cached in it. Values are **1** to **24**.
Maximum Server Threads	Allows you to specify the number of threads ready to serve HTTP requests in the proxy server. Values are **1** to **255**.

3. Press the **Tab** key to save the settings.

Net Link Manager

Net Link Manager is an Enterprise Edge service that provides constant WAN link status monitoring. Net Link Manager is also where you select your WAN primary and backup interfaces.

When Net Link Manager detects a primary WAN link failure, Net Link Manager automatically establishes a backup WAN connection. Net Link Manager monitors the WAN primary link by performing multiple tests. When a predetermined number of tests fails, Net Link Manager establishes the backup connection.

The backup connection uses a V.90 modem (North America) or an ISDN line. When the backup WAN connection is active, Net Link Manager continues to monitor the status of the primary WAN link connection. When the primary WAN link connection becomes available again, Net Link Manager disconnects the backup connection and re-establishes the primary WAN link.

Warning
If an ISDN dial-up connection is used as the primary WAN connection (that is, no permanent WAN connection is configured), no backup link is available.

Note: Net Link Manager can provide backup for one link only, even though there are two primary links (one provided from each WAN interface). Net Link Manager backs up the link who is responsible for the next hop address.

Note: Net Link Manager manages the default route in Enterprise Edge. If a link breaks, Net Link Manager removes all the default routes on the broken link and adds them to the backup link. This happens during switch over from primary to secondary link. The default routes return to the primary link after the connection to the primary WAN link is reestablished.

To enable or disable Net Link Manager:

1. On the navigation tree, click **Services** then click **Net Link Manager**. The Net Link Manager Summary screen appears.

   The Summary screen attributes are:

Attribute	Description
Description	Shows a description of Net Link Manager.
Version	Shows the version number of the subsystem.
Status	Shows the status of Net Link Manager. This box also provides commands to enable or disable Net Link Manager. Possible values: **Up**, **Disabled**, **Enabled** The default value is: **Up**

2. In the **Status** list, select enable or disable.

Selecting the permanent WAN link as the primary WAN connection

1. From the Primary WAN Connection screen, click **Mode** and from the list click **Permanent.**

2. Press the **Tab** key to validate your choice.

3. The Permanent WAN Connection Setting attributes are:

Next Hop on Primary Link	Allows users to enter the IP address (in dot format) of the next hop router which usually is the remote router of the primary WAN link. For more information on setting up remote router, see Appendix C: Setting Up Remote Routers on page 389.
Up Poll Interval	Allows you to set the polling interval, in seconds, when the primary WAN link is operational WAN.
Down Poll Interval	Allows you to set the polling interval, in seconds, when the primary WAN link is down, and the backup (dial-up) WAN link is operational.
Switch Over Delay	Allows you to define the interval, in seconds, that Net Link Manager waits before switching back to the primary WAN link when it becomes available. This delay is to let the router at the other end of the primary link recognize that the primary link has come up and allows for necessary routing table updates. The default value is **30** seconds.
Backup Dial Up Interface	Allows you to select which dial up interface to use.

4. In the **Next Hop on Primary Link** box, type the IP address of the next hop. This address is used by Net Link Manager to add a default route in the Enterprise Edge server. If this address is unreachable, Net Link Manager dials the backup link and changes the default route.

5. In the **Up Poll Interval** box, type the interval value in seconds.
The up poll interval is the interval between successive pings when the next hop on the primary link is available.

6. In the **Down Poll Interval** box, type the down poll interval in seconds.
A short interval provides faster recovery.

7. In the **Switch Over Delay** box, type the switch over delay in seconds.

8. From the **Backup Dial Up Interface** list, select the dial up interface to use for WAN backup.

9. Press the **Tab** key to save the settings.

Selecting a dial-up link as the primary WAN connection

The dial-up WAN connection is always configured as dial-on-demand. The dial-up WAN connection supports PPP only. Enterprise Edge supports ISDN dial-up WAN connection

Note: When you configure your primary WAN connection to use a dial-up WAN connection, no backup WAN connection is available.

1. From the Primary WAN Connection screen, click **Mode** and from the list click **Dialup.**

2. Press the **Tab** key to validate your choice

3. In the Primary WAN Connection Setting section, select a dial-up interface from the **Primary Dial-up Interface** list.

Tips

Before you can select a dial-up interface to connect to the network, you must first create a dial-up interface under **Resources**, **Dial up**. For information on creating a dial-up interface, see Dial Up on page 58.

4. From the menu click **View** then click **Refresh** to save your settings.

Alarm Service

Enterprise Edge Alarm Service performs the following functions:

- Monitors WinNT event logs for incoming event.
- Synchronizes WinNT logs with Enterprise Edge alarm database.
- Receives events (alarms) from other Enterprise Edge applications through its API and logs the events in the Enterprise Edge database.
- Archives alarm history based on the criteria defined in Alarm Manager.
- Monitors the alarm configuration changes and updates SNMP trap agent and Alarm Service.

To configure Alarm Service settings:

1. Choose **Services** and click on the **Alarm Service** heading.
   The Alarm Service Summary screen appears.

2. Configure the Alarm Service Summary screen attributes according to the following table:

Attribute	Description
Descriptions	Shows a description of the alarm service.
Version	Shows the version of the alarm service.
Status	Allows you to enable or disable the alarm service.

3. Press the **Tab** key to save the settings.

NAT (Network Address Translation)

Enterprise Edge provides security and firewall features to protect your private data resources from outsiders. The Network Address Translation feature a network security feature. NAT is the translation of Internet Protocol addresses used within your private network to different IP addresses known to Internet users outside your private network. NAT helps ensure network security because each outgoing or incoming request must go through a translation process that also provides the opportunity to qualify or authenticate the request or match it to a previous request. NAT also translates port numbers.

Enterprise Edge supports both static and dynamic NAT for a number of packet types and protocols:

NAT Support for:	Type
Packets (static and dynamic)	TCP, UDP, IP
Protocols	H.323, FTP, HTTP, POP3, Telnet, SMTP, DNS, TFTP, GOPHER, FINGER, NNTP, RPC, SUNNFS and SNMP

Static NAT

Static NAT is the one-to-one mapping of an IP address on your private network to an IP address from outside your network. Inbound rules must have external IP addresses mapped to specific internal IP addresses.

Dynamic NAT

Dynamic NAT is the mapping, between a private network and the outside network, of one address to a pool of addresses, a pool of addresses to one address or a pool of addresses to another. The mappings are made in a translation table and remain there until the table is cleared or until an entry times out.

To view Summary NAT screen:

1. On the navigation tree click **Services,** then click on the **NAT** heading.
   The NAT Summary screen appears. The Summary screen attributes are:

Attribute	Description
Description	Shows a description of NAT.
Version	Shows the version number of the subsystem.
Status	Allows you to enable or disable NAT. Possible values: **Disabled**, **Enabled** The default value is: **Disabled**

2. Select the status of NAT, **Disabled** or **Enabled**.

3. Press **Tab** to save the setting.

Configuring an Interface with NAT

1. Choose **NAT** to expand the navigation tree and click on the interface you want to configure. For example, **LAN1**.
   The Rule Configuration and Rule Setting screens appear.

   Note: Rules can be configured in one of two ways, using default rules or setting up individual rules.

Adding Default rules

2. Select the status of Default Rules: **Enabled** or **Disabled**. The default is Disabled. Two default rules are set. One is for TCP/UDP and the other for IP. Both are outbound. The IP address for the Public address is the IP address of the interface you configure. The system automatically fills in the rule order. If you choose to add additional rules, the default rules still remain, unless you disable Default Rules.

   Note: Before you can specify the Rule Order you must first add the Rules.

Add a Rule to an Interface

3. Under Configuration, click Add Rule.
   The Rule Setting dialog box appears.

4. Configure the Rule settings according to the following table:

Attribute	Description
Rule Name (R#)	Allows you to assign a number to the Rule.
Direction	Allows you to choose if the direction of the rule is **In**, **Out** or **Both**. **Both** only applies to IP protocols.
Protocol	Allows you to choose the protocol for this interface; **IP**, **TCP**, **UDP**, or **TCP/ UDP**.
Private IP Type	Allows you to specify if the IP type is **Fixed** or **Dynamic**. The default is **Fixed**.
Private IP	Allows you to specify the Private IP address. The Rule is invalid without this IP address.
Private Mask	Allows you to specify the mask to use with the Private IP.
Private Port Range (#-#)	Allows you to specify a single or range of entries (1-65535) or the following; **ALL**, **FTP**, **Telnet**, **SMTP**, **DNS**, **Finger**, **HTTP**, **H.323**, **POP3**, **NNTP**, **RPC**, **SUNNFS, SNMP, SNMP-TRAP, TFTP and Gopher**.
Public IP Type	Allows you to specify if the IP type is **Fixed** or **Dynamic**. The default is **Fixed**.
Public IP	Allows you to specify the Public IP address. This address should be on the outside network.
Public Mask	Allows you to specify the mask to use with the Public IP. If you enter 255.255.255.255 then the Public IP is a single address. If you enter 0.0.0.0 then the Public IP is all possible addresses.
Public Port Range (#-#)	Allows you to specify a single or range of entries (1-65535) or the following; **ALL**, **FTP**, **Telnet**, **SMTP**, **DNS**, **Finger, HTTP, H.323, POP3, NNTP, RPC, SUNNFS, SNMP, SNMP-TRAP, TFTP and Gopher**.

Note: If you do not configure the public and private masks correctly the system will be affected. You must specify addresses that exist. For example, if you configure an outbound rule, the Public IP address and Public Mask are the translated addresses. These addresses must be assigned or packets will be sent to a non-existent destination. For inbound rules, the translated address is the Private Address and Mask.

5. Click **Save**.

6. When you finish adding rules, configure the **Rule Order** box in the Rule Configuration screen for the interface.

   Note: Configure the rule order from most specific to most general. For example, a TCP rule for one port should come before a general rule for all TCP traffic. IP rules should come last.

7. Press **Tab** to update the screen.

Example of a common NAT configuration

An Enterprise Edge has two LANs and a WAN. The WAN connects to the outside and has one public IP address. The LANs are part of a private network. The system allows outgoing traffic but only HTTP traffic is allowed in. LAN1 subnet is 10.10.10.0, LAN2 is 10.10.11.0. The WAN address is 48.123.35.41. The web server address is 10.10.10.4.

The rules would be as follows:

Rule1	Rule 2
Direction: Out	Direction: In
Protocol: TCP/UDP	Protocol: TCP
Private IP Address: 10.10.0.0	Private IP Address: 10.10.10.4
Private IP Type: Fixed	Private IP Type: Fixed
Private IP Mask: 255.255.0.0	Private IP Mask: 255.255.255.255
Private Port Range: All	Private Port Range: HTTP
Public IP Address: 48.123.35.41	Public IP Address: 48.123.35.41
Public IP type: Fixed	Public IP type: Fixed
Public IP mask: 255.255.255.255	Public IP mask: 255.255.255.255
Public Port Range: ALL	Public Port Range: 8080[a]

a. Mapping 8080 to the HTTP port on 10.10.10.4.

IP Firewall Filters

The Enterprise Edge IP Firewall Filters feature is one of the security features Enterprise Edge offers to protect your network against intruders. The security and firewall features are also used for controlling what outside resources your users will be able to access. The following features are part of the Enterprise Edge firewall:

- Basic (stateless) Packet Filter
- Stateful Packet Filters

The DNS proxy also carries security features because it keeps all of the internal IP addresses from external web servers. For information on DNS proxy, see DNS on page 199.

Note: For information on using filters for IPX routing, see IPX Routing on page 208.

Packet filtering

A packet filter is a firewall facility that can monitor the state of active connections and use this information to determine which network packets to allow through the firewall.

Basic (stateless) Packet Filter

Enterprise Edge supports basic (or stateless) packet filtering for IPX protocols. With basic packet filters, you can configure your system to:

- Pass packets only from the routes listed in the filter definition.
- Pass everything except the packets from the routes listed in the filter definition.

To view and change the status of Firewall Filters:

1. Choose **Services**, then click on the **IP Firewall Filters** heading.
   The Firewall Filters Summary screen appears. The Summary screen attributes are:

Attribute	Description
Description	Shows a description of Firewall Filters.
Version	Shows the version number of the subsystem.
Status	Shows the status of Firewall Filters. This box also provides commands to enable or disable Firewall Filters. Possible values: **Disabled**, **Enabled** The default value is: **Disabled**

2. Choose the status of the Firewall Filters, **Enabled** or **Disabled**.

Configuring Firewall Filters for an Interface

3. Choose Firewall Filters and click on the heading you want to configure. For example, **LAN1**.
   The Logging Settings, Log Viewing Options, Input Filters' Rule Configuration, Input Filters' Rule Setting, Output Filters' Rule Configuration, Output Filters' Rule Setting screens appear.

4. In the Logging Settings screen, choose if **Logging** is **Disabled** or **Enabled**.

5. In the Logging Settings screen, choose the **Logging Level**:
   - Level **1** logs errors only
   - Level **2** logs warnings
   - Level **3** logs everything

6. In the Log Viewing Options screen, type the **Start Date** and **End Date** (mm/dd/yyyy).This is only necessary if you wish to view existing logging data.

   Note: You can configure rules two ways; using default rules, or, setting up individual rules.

Adding Default Rules

7. Select the status of Firewall Status: **Enabled** or **Disabled**. The default is **Disabled**. When you enable Firewall Status, the system allows all outgoing packets and blocks all incoming packets. If this is how you want the system to work, then no other rules need to be set.

Adding an Input Filter for a Firewall Filter Interface

8. Before you can specify a Rule Order you must add Filters.
   On the **Configuration** menu click **Add Input Filter** or **Add Output Filter**.

9. Configure the Input/Output Filter according to the following table:

Packet Filter Feature	Comments
Name(IR#)	Allows you to assign a number to the Rule.
Stateful	Allows you to specify if this rule will have its states monitored. This permits the creation of one-way rules. For example, you can permit inside traffic to return but block outside traffic. For more information refer to Stateful Packet Filters on page 238. The values are **Yes** and **No**. The default is **Yes**.
Disposition	Allows you to specify if a packet that matches this rule passes through or is blocked. The values are **Block** or **Pass**. The default is **Block**.
Protocol	Allows you to specify the protocol type of the packet to be filtered. The values are; **IP**, **TCP**, **UDP**, **TCP/UDP** and **ICMP**. The default is **IP**.
Source IP Type	Allows you to specify if the Source IP is **Fixed** or **Dynamic**. The default is **Fixed**.
Source IP	The source address box of the packet to be filtered.
Source Range Mask	Allows you to specify the source address mask of the packet to be filtered. If you enter 255.255.255.255 then the Public IP is a single address. If you enter 0.0.0.0 then the Public IP is all possible addresses.
Source Port Range (#-#)	Allows you to specify a single or range of entries (1-65535) or the following; **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **DNS**, **DHCP**, **TFTP**, **Gopher**, **Finger**, **HTTP**, **H.323**, **POP**, **NNTP**, **NetBios**, **RPC**, and **SUNNFS**.
Destination IP Type	Allows you to specify if the Destination IP Type is **Fixed** or **Dynamic**. The default is **Fixed**.
Destination IP	Allows you to specify the Destination IP address.

Packet Filter Feature	Comments
Destination Range Mask	Allows you to specify the source destination mask of the packet to be filtered. If you enter 255.255.255.255 then the Public IP is a single address. If you enter 0.0.0.0 then the Public IP is all possible addresses.
Destination Port Range (#-#)	Allows you to specify a single or range of entries (1-65535) or the following; **ALL**, **FTP**, **Telnet**, **SMTP**, **SNMP**, **DNS**, **DHCP**, **TFTP**, **Gopher**, **Finger**, **HTTP**, **POP**, **NNTP**, **NetBios**, **RPC**, and **SUNNFS**.
Source Routing	Allows you to specify how Source Routing is checked. **Ignore**: source routing is not checked. **Allow**: packets with source routing are matched. **Deny**: packets without source routing are matched. The default is **Ignore**.
IP Options	Allows you to specify how Source Routing is checked. **Ignore**: IP options are not checked. **Allow**: packets with IP options are matched. **Deny**: packets without IP options are matched. The default is **Ignore**.
Quick	Allows you to specify the order of rule match. Yes means that the first rule match is used. No means the last rule match is used.

Note: By default, there are no packet filters.

10. Click **Save**.

After you enter all the Input and Output Filters for an interface:

11. Type in the Input Filters' Rule Order for the interface you are configuring.

12. Type in the Output Filters' Rule Order for the interface you are configuring.

Stateful Packet Filters

Enterprise Edge supports stateful and basic packet filtering for IP protocols. Stateful packet filters monitor active sessions and records session information such as IP addresses and port numbers. They maintain state information for each flow (TCP, UDP or ICMP). Stateful filters use the state information to determine if a packet is responding to an earlier request from an internal node. If the packet is in response to a request previously made from within the network, the packet is forwarded to its destination. If a packet originates from an external node, it is dropped unless a filter rule specifically allows it to be routed to an internal node.

Stateful packet filters protect your network against Internet attacks such as source spoofing, where an attacker pretends to be a trusted user by using an IP address that is within the accepted range of IP addresses of your internal network. Enterprise Edge stateful packet filtering validates that addresses coming from outside the network are valid outside addresses. Stateful packet filter also protect your network from a denial-of-service attack, where an attacker tries to block valid users from accessing a resource or a server.

Stateful filtering supports TCP, UDP, IP, and ICMP. Stateful filtering supports the following applications: H.323, FTP, HTTP, POP3, Telnet, SMTP, DNS, DHCP, TFTP, GOPHER, FINGER, NNTP, NetBios, POP2, RPC, SNMP and SUNNFS.

Stateful and basic filtering is configured based on the following criteria

Packet Filter Feature	Comments
Source Address	The source address box of the packet to be filtered.
Source Mask	The source address mask of the address to be filtered.
Destination Address	The destination address box of the packet to be filtered.
Destination Mask	The destination address mask of the address to be filtered.
Protocol	The protocol type of the packet to be filtered. Possible values are **TCP**, **UDP**, **ICMP** or **IP**.
Source Port Range	The source port or range of ports of the packet to be filtered. This box applies only if protocol value is TCP or UDP.
Destination Port Range	The destination port or range of ports of the packet to be filtered. This box applies only if protocol value is TCP or UDP.
Rule Order	In a comma separated list format, gives the order in which the filter must apply the rules listed in the Rule Names box.
Rule Name	Define rule name.
Stateful	Select Yes if stateful filtering is required, or No if stateful filtering is not required. Default: **Yes**.
Disposition	Specifies the action to take for the packets matching a filter's criteria. This parameter must be set for each filter. Action to take may be different from one filter to the next. Values are: **Block** or **Pass**. Default: **Block**.
Source Routing	Specifies whether or not to allow any source routing bits in the **IP options** box in the IP header. Values are: **Ignore**, **Allow** or **Deny**. Default: **Ignore**.
Status	Specifies if the system enforces default filter policy of block all incoming and pass all outgoing packets. If you disable status, the system allows packets through. Values are: **Enabled** or **Disabled**. Default: **Disabled**.
IP options	Specifies whether of not to check any IP options are in the packet. Values are: **Ignore**, **Allow** or **Deny**. Default: **Ignore**.
Source IP Type	For static source IP addresses, this box is set to **Fixed**. Otherwise, it is set to **Dynamic** for source IP addresses. Values are: **Fixed**, **Dynamic**. Default: **Fixed**.

Packet Filter Feature	Comments
Destination IP Type	For static destination IP addresses, this box is set to **Fixed**. Otherwise, it is set to **Dynamic** for dynamic destination IP addresses.
Quick	If this box is set to **Yes**, the filter stops matching operation when it locates the first match. If set to **No**, the filter will check the entire list of rules to find all matches and apply the last match. Default: **Yes**.

Note: When you set filters, make sure to allow the flow of packets going to the RPC port (port 135 TCP or UDP) for correct Unified Manager operation.

For IP Firewall Filter configuration information, see IP Firewall Filters on page 235.

Configuring Digital Private Network Signalling System1

6

Note: Throughout this chapter, M7100, M7208, M7310, and M7324 are used to refer to both the M7xxx and M7xxxN telephone sets. For example, M7100 refers to both the M7100 and M7100N set.

DPNSS 1 services

The Digital Private Network Signalling System (DPNSS 1) is a networking protocol enhancement that extends the private networking capabilities of existing Enterprise Edge systems. It is designed to offer greater centralised functionality for operators, giving them access to Enterprise Edge features over multiple combined networks.

Note: The DPNSS feature is dependent on the market profile loaded on your system and whether on not you have a software keycode to enable the feature.

DPNSS 1 allows an Enterprise Edge local node, acting as a terminating node, to communicate with other PBXs over the network. For example, corporate offices separated geographically can be linked over DPNSS 1 to other Enterprise Edge nodes, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Enterprise Edge nodes to function like a private network, with all features of Enterprise Edge accessible.

Tips

Enterprise Edge DPNSS 1 works as a terminating node only.
Enterprise Edge to Enterprise Edge DPNSS is not supported.

DPNSS 1 features can be used on any Enterprise Edge telephone set. On most Enterprise Edge telephone sets, you must use specific keys and/or enter a number code to access the features. For a description of the types of Enterprise Edge sets, see the *Enterprise Edge Feature Programming Telephone Guide.*

DPNSS 1 capabilities

A single Enterprise Edge node, acting as a terminating node on the network, supports the following capabilities over DPNSS 1 lines:

- Direct Dial Inward (DDI) for incoming calls.
- Originating Line Identification (OLI) for incoming and outgoing calls:
  - — For incoming calls, the Calling Line Identification (CLI/CLID) information is displayed to the user on telephone sets with line display (must be configured in programming).
  - — For outgoing calls, the directory number of the originating party is sent out as OLI.
- Terminal Line Identification (TLI) for incoming and outgoing calls. Referred to as Called Line Identification.
- Selective Line Redirect (SLR) and External Call Forward (ECF) implemented on calls between DPNSS 1, and BRI/PRI, DASS2, and Analog lines.
- These remote access features are supported on DPNSS: DDI, line pool access code, destination Codes and remote page feature codes.
- Software Keys; these are required to enable DPNSS 1.

DPNSS 1 features

The following features are available and can be programmed over DPNSS lines:

- Three Party Service
- Diversion
- Redirection
- Call Offer
- Executive Intrusion
- Route optimization
- Message waiting indication
- Loop avoidance

The following parameters can be configured for DPNNS 1 lines:

- Line Type
- Prime set
- CLID set
- Auto Privacy
- Answer Mode
- Auxiliary Ringer
- Full auto Hold

Some features are transparent to the user, but must be programmed to be activated. Others are available for end-user programming at the set. Detailed explanations of these features follows.

Three Party Service

Three Party Service is a DPNSS 1 feature for Enterprise Edge, similar to the Enterprise Edge Conference feature. In fact, using the feature at an Enterprise Edge set is identical in all respects to the Conference feature.

The Three Party Service allows a user, usually an operator, to establish a three-party conference by calling two other parties from one telephone set. Once the connection is made, the controlling party can hang up, leaving the other two connected. The controlling party can even put one party on hold, and talk to the other party.

Note: Enterprise Edge does not support Hold over the DPNSS link itself, which means that the conferenced party on the distance end of the network cannot place a Three Party Service call on Hold.

This feature is basically designed to allow operators to assist in the connection of calls from one main location.

Making a conference call

To initiate or disconnect from a conference call on an Enterprise Edge system over DPNSS 1, proceed as in “Creating a conference call” in the *Enterprise Edge Feature Programming Telephone Guide*.

Note: Three Party Service is supported on M7100 and M7000 telephone sets, but in a receive-only fashion. These set types cannot initiate Three Party Service. For more information about these set types, see the *Enterprise Edge M7000 User Card* and the *Enterprise Edge M7100 User Card.*

Diversion

Diversion is a DPNSS 1 feature for Enterprise Edge that lets users forward their calls to a third party on the DPNSS 1 network. Functionality is similar to Call Forward on Enterprise Edge, but takes advantage of the broader capabilities of DPNSS.

There are five variations of Diversion: Call Diversion Immediate, Call Diversion On Busy, Call Diversion On No Reply, Bypass Call Diversion, and Follow-me Diversion, described as follows:

- Diversion Immediate diverts all calls to an alternate set. This function is programmed by the user at the telephone set.
- Diversion On Busy diverts all calls to an alternate set when a set is busy. This feature is programmed in the Unified Manager.

- Diversion On No Reply diverts calls that go unanswered after a specified amount of time. This feature is programmed in the Unified Manager.
- Bypass Call Diversion overrides all Call Forward features active on a set over a DPNSS line. An incoming call to the set will not be forwarded; instead, the set will continue to ring as if Call Forward were not active. This feature could be used to "insist" that a call should be answered at that location. Bypass Call Diversion is a receive-only feature on Enterprise Edge, and cannot be invoked from an Enterprise Edge set.
- Follow-me Diversion is also a receive-only feature. It allows the Call Forwarded destination to remotely change the Enterprise Edge Call Forwarding programming (Call Forward All Calls (CFAC) feature) to a different telephone set. (Enterprise Edge CFAC must be active and the destination set/PBX must support the feature.)

  For example, user A forwards all calls to set B, a temporary office. Later, user A moves on to location C. The user does not have to be at set A to forward calls to location C. Using set B and Follow-me Diversion, the user can forward calls from A to location C instead.
- Follow-me diversion can also be cancelled from the forwarded location.

Note: Diversion on Busy and Diversion on No Reply cannot be cancelled from the nominated (forwarded) telephone sets. These are programmable only by an installer and not by the user (as in Diversion Immediate).

Note: If multiple sets are programmed to take a call, the first set to respond will act. All other sets responding are ignored. Therefore, if the first set to respond has Diversion enabled, this feature will be invoked.

Restrictions by set type

Diversion is indicated differently on different types of sets:

- All variations of the feature are supported on Enterprise Edge terminals M7000, M7100, M7208, M7310 and M7324.
- ATA—All variations of the feature are supported on an ATA.
- ISDN—All variations of the feature are supported on ISDN sets except Diversion on Busy and CFWD Busy.
- Portables—All variations of the feature are supported on portable sets.
- DNA—Diversion features can be invoked from an Enterprise Edge set connected on a DNA with boot up. This set can act as a valid destination for DPNSS Diversion regardless of whether a set is physically connected to the DNA.

Setting Diversion

You set Diversion for DPNSS in the same way as Call Forward, see Capabilities on page 98. You will need to enter the end DN when prompted. You may also need to include the DPNSS 1 routing number.

Redirection

Redirection is a DPNSS 1 feature similar to Enterprise Edge Transfer Callback. Redirection lets a call awaiting connection, or re-connection, be redirected by the originating party to an alternate destination after a time-out period. Failed calls can also be redirected. Priority calls are not redirected.

Note: The address to redirect depends on the history of the call. Calls that have been transferred could be redirected to the party that transferred them. In all other cases, the address to redirect is the one registered at the PBX originating the redirection.

Note: Enterprise Edge does not support the redirection of Enterprise Edge originated calls, even over DPNSS 1.

The Diversion on No Reply feature takes precedence over Redirection.

Restrictions by set type

Redirection is indicated differently on different types of telephone sets:

- For sets without displays the "#" key acts as MORE and the "*" key acts as VIEW.
- ATA—Is not supported.
- ISDN—All variations of the feature are supported on ISDN sets.
- Portables—All variations of the feature are supported on portable sets.
- DNA—Is not supported.

Setting Redirection

The timer used for the network Callback Feature applies for redirection.

Executive Intrusion

Executive Intrusion (EI) is a DPNSS 1 feature that allows an operator, or other calling party, to intrude on a line when it is busy. This feature might be required, for example, in times of emergency or to make an important announcement when the recipient is on another call.

EI is similar in functionality to Enterprise Edge Priority Call. It is, however, a receive-only feature on Enterprise Edge sets; that is, EI cannot be initiated from an Enterprise Edge set. The originating caller would be on another PBX on the DPNSS 1 network.

When EI is used to intrude on a call in progress, a three-way connection is established between the originating party and the two parties on the call. The result is very much like a conference call. When one of the three parties clears the line, the other two remain connected, and EI is terminated.

Restrictions by set type

Executive Intrusion is indicated differently on different types oftelephone sets:

- ATA—Is supported.
- ISDN—Is not supported.
- Portables—Is not supported.
- DNA—Is not supported.

The set receiving the intrusion will display `Intrusion Call.` A warning indication tone will sound after intrusion has taken place, and the standard conference call tone will sound every 20 seconds.

Intrusion levels

Whether or not a set will accept or reject an Executive Intrusion request depends on the level of intrusion protection programmed. Each set (DN) has an Intrusion Capability Level (ICL) and an Intrusion Protection Level (IPL) of 0 to 3 (Low, Medium and High).

When the ICL of the intruding set is higher than the IPLs of *both* sets on the active call, EI will occur. It is assumed that the intruding set always has a higher ICL, as it will not be an Enterprise Edge set. For this reason, it is best to set the IPLs of most telephone sets to the default of **None**, or Low or Medium.

Intrusion levels are described as follows:

- ICL: determines the set's ability to intrude. As long as the ICL is higher than the wanted party, EI is allowed. Since EI is a receive-only feature, the ICL is not an issue, and in fact cannot be set on Enterprise Edge.
- IPL: determines the set's ability to refuse intrusion. If the IPL is lower than the originating party, EI is allowed. For general purposes setting the IPL to None, Low or Medium is recommended, unless intrusion is not wanted.

To program IPL on a set:

1. Choose **Services**, **Telephony Services**, **Terminals & Sets, Capabilities**.
2. Choose **Intrusion**.
3. Click a Protection level: None, Low, Med, or High.

   If the level of intrusion protection is set to High no intrusions will be allowed. The default is None.

Call Offer

Call Offer over DPNSS 1 allows a calling party to indicate to the wanted party that there is an incoming call available, even though there is no answer button available to present the call on the set. The intended recipient can ignore, accept, or decline the offered call. Call Offer is useful in increasing the call-coverage capability of an Enterprise Edge system, and helps to lift the network processing load. It is a receive-only capability on Enterprise Edge: incoming calls would be initiated at another PBX on the DPNSS 1 network.

An example of Call Offer in use is an operator or attendant who has a number of calls coming in at once. The operator can extend one call and move to the next without waiting for the first call to be answered.

Displays

When a Call Offer is made by the originating exchange, the target set displays a message, and a tone is heard. When an offered call arrives on sets with line display, the user will see `XX...X wtng` if the calling party ID is available and CLID is enabled, otherwise, `Line XXX waiting` is shown (the line name associated with the call). If there are more than 11 digits in the incoming number, only the last 10 will display.

If Call Queuing is programmed for the system, the display will show `Release Line XXX`.

This is the line name of the highest-priority queued call if it is an offered call.

Restrictions by set type

Call Offer is indicated differently on different types of sets:

- M7000—The associated LED or LCD will flash, and a tone is heard.
- ATA—Call Offer is supported as a Camp On feature and a tone is heard.
- ISDN—Is not supported.
- Portables—Is not supported.
- DNA—Is not supported.

Note the following general conditions and restrictions:

- DND on busy must be programmed as N (see Terminals & Sets, Capabilities) for a set to accept Call Offer.
- If CF on busy is programmed for the set, Call Offer will not be accepted.
- The target line for the set must be set to: If **busy: busy tone**, which is the default (see Trunk/line data on page 111).
- Call Offer will not work if sent over Manual answer lines. Again, it is recommended that for the majority of purposes, lines be left at the default: **Auto**.

User Actions

The party receiving a Call Offer has three choices, as follows:

- Ignore it. After a programmed time interval, the Offer request will be removed.
- Reject it. If the user activates Do Not Disturb on Busy (DND) when the Call Offer request is made, the request is removed from the set. The calling party is informed of the rejection.

  A call cannot be offered to a set with DND active. The line indicator for external incoming calls still flashes.
- Accept it. The Offer is accepted by releasing the active call.

Note: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

Route Optimization

Route Optimization is a DPNSS 1 feature for Enterprise Edge that lets calls follow the optimum route between two end PBXs. This allows efficient use of network resources.

Route Optimization is initiated by the system and is transparent to the user. However, in some cases the user may see a call switch from an appearance on the set to another appearance key or from an intercom key to the appearance key or vice versa. This occurs when Enterprise Edge receives a Route Optimization request and initiates a new call to follow the optimal route.

If a set is active on a private line call, the Route Optimization call being established may go on a public line. This will cause a loss of privacy on that line.

Data calls are rejected by Route Optimization in order to ensure the data transmission is not affected.

Certain situations result in Route Optimization not taking place. For example, calls that are using Hold, Parking or Camp features will not undergo Route Optimization, and if a Route Optimization call undergoes Diversion, the Route Optimization is dropped.

Setting Route Optimization

There is no system programming required for the feature when Enterprise Edge is working as a terminating PBX; however, Enterprise Edge must have a private access code programmed that maps to a valid destination code or line pool code on DPNSS lines. Further, Allow redirect must be set to **Y**. For more information, see Capabilities on page 98.

Message Waiting Indication

Message Waiting Indication (MWI) is a DPNSS 1 feature for Enterprise Edge Call Services. Messages are received at a centralised location (a telephone set you pre-determine), where they are processed and forwarded to the target set. This centralisation relieves the network processing load, making the system more efficient. MWI provides users with the ability to scroll through, erase and reply to messages.

When there are messages to be retrieved, `Message for you` is displayed at the set. Once all the messages are retrieved by the user, a Message Waiting Cancellation (MWC) is sent from the call centre, and the user set no longer displays MWI.

MWI also allows the user to reply or call back to the message centre. The procedure for retrieving messages is described in the *Enterprise Edge Feature Programming Telephone Guide*.

This feature is only supported on Enterprise Edge target lines.

Restrictions by set type

- Message Waiting Indication is indicated differently on different types of sets:
- M7000—Ihe associated LED will flash.
- ATA—Is not supported.
- ISDN—Is not supported.
- Portables—Is not supported.
- DNA—Is not supported.

Setting Message Waiting Indication

To set Message Waiting Indication, the following conditions must be established:

- Assign message centre to a line.
- Select message centre for use.
- Assign the line to a set to Appear and/or Ring.

Assigning message centres to a line

You need to assign any one of five, or None, of the message centres to the line. There can be as many as five message centres in a network; that is, five telephone sets on the Enterprise Edge system can act as mailboxes in the message centres offered by five different PBXs on the network. These PBXs may also be from different manufacturers.

Thus, for each message centre there may be different:

- numbers to be dialled to reach the mailbox from the set
- MWI strings received, indicating that the centre has a message in the mailbox

- MWC strings received, indicating that the voice mails have been retrieved

When assigning message centres, you can program all three parameters for each. Remember that the following procedure is not to select a message centre, but to program any or all of the five available message centres. (This is similar to the Direct Dial functionality.)

Tips

The MWI and MWC strings used in this procedure are default NSI strings for Message Waiting.

*58B*AN*1# – Message Waiting Indication
*58B*AN*0# – Message Waiting Cancellation

This provides the information required to program the strings as:

AN*1# for MWI, and
AN*0# for MWC

Private network strings will differ with different message centres. These should only be changed on the advice of your customer service representative.

1. Choose **Services**, **Telephony Services**, **Lines, Telco Features**.

2. Click **Voice message centre numbers**.

3. Choose a Voice message center: **1** to **5**.

   The existing set (DN) for Message Waiting is displayed, if available, as **Tel#:XXXX**.

4. Type the new target number (starting with an access code, if required), or **None**. For example: **65142222**.

   The display shows **MWI:AN*1#**. This is a string sent by the PBX holding the message centre.

5. Program the number that the user will dial on the IC key to retrieve a message from the messaging centre.

6. Program the Non-Specified Information (NSI) string for the MWI that is expected from the particular message centre.

   The display shows **MWC:AN*0#**. See the next procedure: “Programming MWI and MWC.”

7. Program the NSI string for the MWC that is expected from the message centre.

   Note: The line must be programmed to Appear and/or Ring at the set.

Programming MWI and MWC

MWI and MWC information is received from the network in the form of NSI strings. The NSI strings in DPNSS are dependent on the supplier of the PBX; therefore, the strings vary depending on the originating PBX.

Each string has the following default structure:

58XYYYYY..

The table describes each part of the NSI string:

String Component	Description
*58	Identifies that it is an NSI string.
X	Any letter from A to Z, or nothing.
YYYYY..	Manufacturer specific string, which can contain any sequence of alphanumeric digits, or *.
#	Marks the end of the identifier.

Only the YYYYY.. # portion of the string must be programmed for MWI and MWC. The procedure is similar to Set Name/Line Name.

Note: The following criteria must be met when programming NSI strings for MWI/MWC:

- No spaces are allowed, including spaces at the end of the string.
- A # must be present at the end.
- A # or a * cannot be present in the first character.

Selecting a message centre

With a message centre programmed on a selected line, you must set the message centre for use:

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Click a target line number (Line 241 to 364).
3. Click **Telco Features**, **Voice message center numbers**.
4. Choose a Voice Message center: **1** to **5**.

Setting Message Waiting Indication

1. Ensure that you have programmed a set to access target lines for receiving messages (see “Assigning message centres to a line, above):
2. Choose **Services**, **Telephony Services**, **Terminals & Sets.**
3. Click a DN (DN 221-528).

4. Choose **Telco Features**, **Feature assignment**.

5. Click **Y** to enable Call log set.

6. Click **Y** to enable Vmsg set.

   When Vmsg is enabled for a target line on a set, the set logs Message Waiting Indication/Cancellation received for the corresponding target lines to the user.

Loop avoidance

Errors in the configuration of a network may make it possible for a call to be misrouted, and arrive at a PBX through which it has already passed. This would continue, causing a loop which would eventually use up all of the available channels. The Loop Avoidance service permits counting of DPNSS 1 transit PBXs and rejecting a call when the count exceeds a predetermined limit.

Programming Loop avoidance

To set Loop avoidance during hardware configuration:

1. Choose **Resources, Media Bay Modules**, **Bus 02 - 07**, **Modules on Bus, Module 1.**

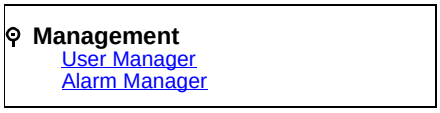
2. Choose **Module type DPNSS**.

3. Type a value (0-25) in the Maximum transits box.

   The default value is 25.

Configuring Management Settings 7

The following shows the programming map for **Management**:



In Enterprise Edge Unified Manager, **Management** allows you to manage user and alarm settings. Under the **Management** heading, Unified Manager displays the following subheadings:

- **User Manager**, which displays the User Profile window showing a list of the current Enterprise Edge user name and associated passwords and access privileges. The User Profile window allows you to add, modify or delete any user profile information.
- **Alarm Manager**, which displays the Alarm Database, SNMP Trap and the Alarm Backup Batch Job windows. The Alarm Database window allows you to modify event information collection parameters. The SNMP Trap window allows you to enable or disable the sending of different SNMP traps. The Alarm Backup Batch Job window allows you to enable or disable and to schedule alarm backup batch job.

User Manager

Enterprise Edge comes with the following default user profiles:

- **Manager** Default password: "manager". Access privilege: Read-Write
- **ModemBackup (North America only):**
- **supervisor: administrator type user, with "visor" as the default password**
- **TivDialup**:
- **user**: read-only type user, with "user" as the default password

Note: After installation, change the all administrator type passwords.

WARNING

Do not change the default ModemBackup and TivDialup passwords. If you change the TivDialup password, Enterprise Edge cannot connect with Tivoli. If you change the ModemBackup password, Enterprise Edge cannot make a dialup network connection if NetLinkManager detects a break in the permanent link.

Adding a user profile

To add a user profile:

1. From Unified Manager, select **Management, User Manager**.
   The User Profile screen appears showing the current user profile information.

2. From the **Configuration** menu, select **Add User**.
   The User Profile dialog box appears.

3. Use the following table to add the new user profile information:

Attribute	Description
User Name	Allows you to enter the user name. The User Name is case-sensitive and must not exceed 50 characters in length.
Password	Allows you to assign a password for the user. The password is case-sensitive and must exceed 15 characters in length.
Confirmed Password	Allows you to enter the password again to validate the new or modified password.
Privilege	Allows you to select the level of access associated with the user name. The following levels of access are available: READ-ONLY: Allows you to view programming settings, but not to modify them. READ-WRITE: Allows you to view and modify programming settings. READ-WRITE-DIAL: Allows you to view, modify and use a network dial-up connection. READ-ONLY-CDR: Allows you to view CDR programming settings. READ-WRITE-CDR: Allows you to view and modify CDR programming settings.

4. Click the **SAVE** button to save your settings.
   The new user profile information is added to the list on the User Profile window.

Modifying a user profile

To modify a user profile:

1. From Unified Manager, select **Management, User Manager**.
   The User Profile window appears showing a list of the current user profiles.

2. From the User Profile window, click on the User Name for which you want to modify user profile information.
   The row containing that user profile information is highlighted.

3. From the **Configuration** menu, select **Modify User**.
   The User Profile dialog box appears.

   Note: You cannot modify a user name. You must delete the complete User Profile row from the User Profile window and add a profile with the new name.

4. Make the necessary changes in the User Profile dialog box.

5. Click the **SAVE** button to save your settings.
   Unified Manager displays the User Profile window.

Deleting a user profile

To delete a user profile:

1. From Unified Manager, select **Management, User Manager**.
   The User Profile window appears showing a list of the current user profiles.

2. From the User Profile window, click on the User Name you want to delete.
   The row containing the user profile information is highlighted.

3. From the **Configuration** menu, select **Delete User**.
   A Select an Option dialog box asks you if you want to delete this row.

4. Click the **YES** button to delete the user profile.
   The User Profile window is updated.

   Note: Maintain only one user profile with administrator privileges and allow only system administrator to use this user profile. Multiple users logging on to Enterprise Edge from different client stations using the administrator account can cause inconsistent or wrong configuration.

Alarm Manager

The Alarm Manager enables you to manage the collection and storage of alarm information. The Alarm Manager allows you to set different collection parameters for the Alarm Database. You can use the Alarm Manager to enable or disable the sending of all or some types of SNMP traps. The Alarm Manager provides the Alarm Backup Batch Job, an application which backs up old alarm records to an archive folder at a scheduled time.

Enterprise Edge provides real-time information about what is occurring within the Enterprise Edge system through the Alarm Banner and the Alarm Browser.

The Enterprise Edge alarm system includes the following components:

- Alarm Banner: The Alarm Banner provides a window which allows you to continually monitor the Enterprise Edge system for alarms. For more information, see Fault Alarm Banner on page 308.
- Alarm Browser: The Alarm Browser allows you to browse through a list of alarms and provides detailed information on each one. For more information, see Alarm Browser on page 308.

Configuring the Alarm Manager

1. From Unified Manager, click the **Management** key to expand the navigation tree and then click **Alarm Manager**.
   Unified Manager displays the Alarm Database, SNMP Trap and Alarm Backup Batch Job windows.

2. Use the following table to configure the Alarm Database:

Attribute	Description
Maximum Number Record	Allows you to set the maximum number of records that the alarm database stores. The default is 0 (no limit). The range is from 0 to 5000.
Kept Timer (days)	Allows you to set the number of days that the records remain in the database before the record is archived.
Resync Timer (seconds)	Allows you to set, in seconds, the interval (in seconds) at which the alarm service synchronizes with the Windows NT event logs.
Archive Location	Allows you to enter the path to the directory where the alarm information is kept. The default path is: “d:datafiles\nortel networks\unified manager\archive\

3. Click **TAB** to save your settings or continue the configuration.

4. Use the following table to configure the SNMP Trap:

Attribute	Description
TrapsEnabled	Allows you to enable or disable the sending of SNMP traps when a new event arrives in the alarm database.
EventInfo Enabled	Allows you to enable or disable sending SNMP traps when an “Information” event arrives in the alarm database.
EventWarning Enabled	Allows you to enable or disable sending SNMP traps when a “Warning” event arrives in the alarm database.
EventError Enabled	Allows you to enable or disable sending SNMP traps when an “Error” event arrives in the alarm database.
SrcExclusion List	Allows you to add, in a comma-separated format, a list of event sources from which SNMP traps must not be generated. The source exclusion list prevents you from receiving SNMP traps which have no meaning to you.

5. Use the following table to configure the Alarm Backup Batch Job:

Attribute	Description
Batch Job	Allows you to start or stop a scheduled batch backup to an archive folder. The Alarm Backup Batch Job uses the Kept Timer value from the Alarm Database screen to determine when to archive an alarm record.
Schedule Day	Allows you to set the day when the system must perform the backup.
Schedule Time	Allows you to set the time the backup must start.

Tips

Before you change the day or time, or both, you must first stop the batch job. Make your changes, and then start the batch job again.

Maintenance 8

This chapter contains the following information:

- Enterprise Edge general maintenance on page 259
- Enterprise Edge system diagnostics and utilities on page 269
- Maintenance programming for telephony resources on page 278

For information on hunt group and call-by-call usage metrics, refer to Metrics on page 301.

For information on physically moving telephones, refer to Moving telephones on page 302.

Enterprise Edge general maintenance

- System startup on page 259
- Warm reset on page 260
- Backup and restore on page 260
- Backup, restore, upgrade utility (BRU) for Enterprise Edge system on page 261
- Backup and restore telephony programming using Unified Manager's Tools menu on page 265

System startup

A system startup replaces any existing telephony programming with the default programming.

1. Choose **Diagnostics**, **MSC**.

   The **Configuration** menu is enabled.

2. Access the **Configuration** menu and click **System startup**.

   The system displays a dialog box with three parameters: **Region**, **Template** and **Start DN**.

3. Select a region from the **Region** list: **Global**, **UK** (United Kingdom), **Sweden**, **Holland**, **CALA** (Central America Latin America), Carib (Caribbean), **NA** (North American) or **Denmark**.

Each region has a Market Profile associated with it. For more information on Market Profiles, refer to Appendix D: Market profile attributes on page 391.

Note: When you select a new region, the Template list is read-only. It is only after the system is restarted that the available templates for this region are displayed.

4. Type any valid value in the **start dn** box. The box displays the current value.

5. Click **OK** to apply these changes.

   The system displays a warning that the system will restart and default programming values will be restored.

   Note: After the system's cold start is completed, you can use a different template than the default template. From **Diagnostics**, **MSC, System startup** and select a template from the template list. However, if you select a new template, you must perform another system restart.

Warm reset

A warm reset restores the system but does not affect the current telephony programming.

1. Choose **Diagnostics**, **MSC**. The Configuration menu option is enabled.

2. Access the Configuration menu and click **Warm reset**.

   The system displays a warning that all active calls will be dropped.

3. Click **OK** to continue.

Backup and restore

There are two modes of backup and restore on the Enterprise Edge system; the BRU utility and the Backup and Restore tools which you access through Unified Manager.

The BRU utility manages local, remote and Web-enabled Enterprise Edge software. BRU works with *.xml* script files to perform step-by-step backup, restore or upgrade of the full Enterprise Edge system or selected components. After you select the needed components, BRU creates a ready-to-run Windows NT script file which BRU can execute immediately or at a repeatable scheduled time and date.

Unified Manager's Backup and Restore tools allow you to back up your telephony programming or retrieve a complete copy of telephony programming information to restore on the Enterprise Edge system.

For more information on backing up and restoring your Enterprise Edge system programming, refer to the following:

- Backup, restore, upgrade utility (BRU) for Enterprise Edge system on page 261
- Backup and restore telephony programming using Unified Manager's Tools menu on page 265

Backup, restore, upgrade utility (BRU) for Enterprise Edge system

BRU provides additional functionality that complements the Unified Manager telephony programming backup and restore features.

You launch the BRU utility after starting a virtual network computing (VNC) session. The VNC desktop sharing utility supplied with Enterprise Edge allows you to access the desktop of the Enterprise Edge server from another computer. For more information on VCN, refer to *Enterprise Edge Installation and Maintenance Guide*.

BRU is used to backup the system registry and customer data stored by default on the Enterprise Edge hard disk drive. You can store a backup file on any network accessible drive.

The Enterprise Edge system includes two default script files; Backup and restore and Upgrade. For more information, refer to:

- Building Windows NT script files on page 261
- Starting BRU on page 262
- Performing a backup or restore using BRU on page 262

Building Windows NT script files

BRU creates a Windows NT.*cmd* file from the information retrieved from the.*xml* file and data from user input. The assembled *.cmd* file is then executed. In order to create a backup, restore or upgrade script, BRU must first load the corresponding *.xml* file.

Each *.xml* file contains a top level section that lists the main sections in the *.xml* file with for example, tasks such as BACKUP or RESTORE. For each of these tasks there is a list of available components.

The *.cmd* file is built from selections from the list of available components. Once the component is in the Selected Components window, BRU reads the instructions for this component and writes the *.cmd* file. BRU can execute the file immediately or at a specified time and date on a Once, Daily, Weekly, or Monthly schedule.

Starting BRU

Use the following procedure to start a BRU session.

1. From your browser, log into your Enterprise Edge system by entering its IP address and specify port 5800. For example, if your system's IP address is 47.20.112.167, enter 47.20.112.167:5800.

   The system prompts you for a password.

2. Enter the default password *TeirGR8*.

   Note: The system administrator must change this password after the system is installed.

3. At this point, you can set the VNC options to the most reliable operation by selecting the **Options** menu and setting parameters within the Options window.

4. On the remote desktop choose **Start**, **Programs**, **Nortel Networks, BRU**.

   The EE Backup/Restore/Upgrade window appears.

Performing a backup or restore using BRU

After you have BRU running, use the following procedure to perform a backup or restore.

WARNING

When you perform a restore, you must always use the same method as the one you choose to create your latest telephony programming backup file. For example, if you used BRU to perform your latest telephony programming backup, use the BRU utility to restore your programming.

1. Click **Load** to select and load an *.xml* script file.

   A number of backup *.xml* script files are provided with the Enterprise Edge system. In addition, there are upgrade script files provided which are used to upgrade the core software. For more information on *.xml* script files, refer to Viewing the created scripts on page 264.

2. Choose the *EE BR.xml* file from the **Open** dialog box.

3. Click **Open**.

4. From the **Mode** list, select **Backup** or **Restore**.

> ***WARNING***
> When a telephony programming backup is in progress, voice applications stop working. Enterprise Edge maintains call processing service.

> ***WARNING***
> When the telephony programming restore is in progress, Enterprise Edge voice applications and call processing stop working. You must plan telephony programming restore carefully to minimize impact on Enterprise Edge users.

5. From the **Available Components** box, select the component(s) you want to backup or restore. Available components are:

   - **Voice Apps Data**: includes the contents of all the mail boxes as well as the Voice Mail setup information.
   - **RRAS** (Routing and Remote Access Server): contains the configuration of the routing and remote services.
   - **Web Server/TAPI**: includes the Apache Web server, the TAPI configuration files and Unified Manager settings.
   - **Registry**: this is the Windows NT system registry. It includes system registry and user setup information.
   - **Telephony**: includes all telephony programming.
   - **Selective**: allows user to backup any drive or directory.

   Note: It is considered good practice to perform a full backup (select all of the available components except Selective).

   Note: Always backup the Registry component along with any other component you want to backup up. The Registry component.

6. Click the right arrow button to move the component to the **Selected Components** box.

7. Click **Execute** to run the Backup or Restore file immediately,

   or

   If you would like to run the Backup tool at another time, select the check box under **Schedule** and:

   a. Deselect the **Current time** check box.

   b. Use the arrow keys to set the time of execution.

   c. From the **Date** box, select the date.

8. From the **Execute** list, select how often you want to execute the backup operation (Once, Daily, Weekly, Monthly).

9. At this point, you can click the **Execute** button to run the file and the file runs at the time you have indicated.
   After you click **Execute**, the system displays a **Browse for Folder** window.

10. Select a folder. If you are doing a backup, indicate where you want to store your backed up files. If you are doing a restore, indicate the directory from which you are restoring files.

    Note: BRU requires that the destination folder be a mapped or physical drive and it will prompt you to map the folder to a drive.

11. Click **OK**.
    The status indicators show that the script has been created. The estimated time to complete the script is displayed. For more information on script schedules, refer to Viewing the BRU schedule on page 265.

    Note: Because the script is stored in the Temp directory, you must exercise caution when clearing your Temp directory.

Viewing the created scripts

You can view the *.cmd* file using the following procedure:

1. After you have loaded the *.xml* file, select the **View Script** option in the Backup/Restore/Upgrade window.

2. Use the arrow key to move the component(s) in the **Selected Components** box.

3. Click **Execute**.
   The **Browse for Folder** window is displayed.

4. Choose a source drive and click the **OK** button.

5. A BRU dialog box asks if you want to view the *.cmd* file for the selected component and instructs you to close any sessions of Notepad.

6. Click the **YES** button to view the *.cmd* file.
   Notepad is launched with the script displayed. You may edit the file at this point.

7. Close the Notepad window.
   A BRU dialog box asks if you are ready to execute the file

8. Click the **Yes** button if you wish to proceed.

Viewing the BRU schedule

If you would like to verify the BRU schedule use the following procedure:

1. Open the Command Prompt window by choosing **Start**, **Programs**, **Command Prompt**.

2. Type the WinNT command 'at'.
   This command displays the schedule when each script will run and the script file name.

Backup and restore telephony programming using Unified Manager's Tools menu

Unified Manager's Backup and Restore tool allow you to back up the telephony component of your Enterprise Edge system programming. The Restore option allows you to retrieve and apply a complete set of previously backed up telephony programming information to an Enterprise Edge system.

If a backup file becomes damaged, you cannot retrieve the programming information. Equip the device where you store your backup files with an application that protects files from computer viruses and performs file backup and encryption.

The Backup and Restore tool stores two different copies of system programming: a current backup copy and an archive backup copy.

- Fnvram.NEW is the current backup copy. This file contains the result of the latest telephony programming backup. By default, the restore process retrieves the programming information from that file.
- Fnvram.OLD is the archive backup copy. This file is the result of the second last telephony programming backup.

You cannot change the names of the programming backup files. If you need to create other versions of the backup files, you must create additional folders. Backup files are treated like an assembly line. When a successful backup is performed, the information stored in the current backup file is moved to the archive backup file.

Refer to the following procedures for more information:

- Performing a telephony backup using Unified Manager's Tools menu on page 266
- Performing a telephony restore on page 266
- Stopping a telephony backup on page 268
- Stopping a telephony restore on page 268

Note: The Backup, Restore, Upgrade utility (BRU) provides additional functionality that complements the Unified Manager telephony programming backup and restore tool. BRU works with *.xml* files to perform step-by-step backup, restore or upgrade of the full Enterprise Edge system or selected components. For more information, refer to Backup, restore, upgrade utility (BRU) for Enterprise Edge system on page 261.

Performing a telephony backup using Unified Manager's Tools menu

When you perform a backup, the telephony component of your system slows down. Plan to perform a backup when you don't need your system for other tasks.

Use the following procedure to perform a backup.

1. From Unified Manager, click the **Services** key to expand the navigation tree and then click **Telephony Services**.

   Unified Manager enables the **Tools** menu and displays the Backup/Restore options screen. The Backup/Restore Path box shows the default path where telephony backup files are stored. The default path is d:\Data Files\Nortel Networks\Voice Solution\Backups.

2. From the **Tools** menu, choose the **Backup** option.

   A confirmation dialog is displayed, asking if you wish to start now.

3. Click **Yes** to start.

   When a backup is in progress, the text shows the current action and the file name. For example, "Backing up System Programming into file Fnvram.new." When a backup is in progress, a bar graph shows the rough percentage of the action that is complete.

Note: When a backup is in progress, you can click **Cancel** to discontinue the operation. For more information, refer to Stopping a telephony backup on page 268.

4. When the backup is complete, click **Done**.

   The Backup and Restore dialog box closes.

Performing a telephony restore

The Restore feature allows you to overwrite existing programming. When you perform a restore, the telephony component of your system is non-operational and call processing is suspended. Perform restores during non-business hours, and warn users that the Enterprise Edge system will be out of service. Schedule restores for a time when you don't need your server for other tasks.

When you run a restore, all of the sets are put in maintenance mode. Programming data from your server's hard disk or other data storage medium is then loaded into the system's memory. After the data is loaded, the Backup and Restore tool takes the sets out of maintenance mode by initiating a warm start. A warm start restarts the Enterprise Edge system with all its programming intact, including any changes you have made.

Use the following procedure to perform a restore..

WARNING
When you perform a restore, you must always use the same method as the one you chose to create your latest telephony programming backup file. For example, if you used BRU to perform your latest telephony programming backup, use the BRU utility to restore your programming.

A restore overwrites existing programming
You cannot recover Enterprise Edge telephony system programming that has been overwritten.

If a restore fails, the system initiates a cold start
If a restore fails to complete due to an error, the system will initiate a cold start. This means that all programming will be lost, and all programming settings will be returned to the factory defaults.

Ensure the restore is completed successfully
A restore replaces all existing programming for the Enterprise Edge system. A failed restore can shut down the Enterprise Edge system and telephone service to a site, so it is important to ensure the restore is completed successfully.

1. From Unified Manager, click the **Services** key to expand the navigation tree and then click **Telephony Services**.

   Unified Manager enables the **Tools** menu and displays the Backup/Restore options screen. The Backup/Restore Path box shows the default path where telephony backup files are stored. The default path is d:\Data Files\Nortel Networks\Voice Solution\Backups.

2. From the **Tools** menu, choose the **Restore** option.

   A confirmation dialog is displayed, asking if you wish to start now.

Note: If you restore any programming which has been enabled by software keys, you may have to re-enter the keys after the restore.

A confirmation dialog is displayed, asking if you wish to start now.

3. Click **Yes** to start.

   When you initiate a restore, there is a period of a minute or longer while the restore action is initiated. When a restore is in progress, the text shows the current action and the file name. For example, “Restoring System Programming from file Fnvram.new.” The system also displays the percentage of programming that has been restored.

   When the restore is complete, the system automatically restarts.

Note: When a restore is in progress, you can click **Cancel** to discontinue the operation. For more information, refer to Stopping a telephony restore on page 268.

4. Verify the system is working properly once the restore is complete.

Stopping a telephony backup

1. When the backup is in progress, click **Cancel** to discontinue the operation.

   The **Close Application** dialog box appears. The backup continues behind the dialog box until you respond.

2. Click **Yes** to stop the backup.

   If you click **No**, the backup will continue.

Stopping a telephony restore

If you stop a restore, you must perform another, successful restore or the system will initiate a cold start. This means all programming will be lost and all settings will return to the factory defaults.

1. When the restore is in progress, click **Stop** to discontinue the operation.

   The **Stop Restore** dialog box appears.

2. Click **Yes** to stop the restore action.

   If you click **No**, the restore action continues.

3. If you select **Yes**, the **Cold Start Warning** dialog box appear saying that the system will initiate a cold start. You can only click **Exit Application.**

4. Click **Exit Application**.

Enterprise Edge system diagnostics and utilities

This section provides information about Enterprise Edge diagnostic programs and utilities including:

- Enterprise Edge Performance Statistics
- Error Messages
- MIB II Information
- Alarm Banner
- Alarm Browser

Performance Statistics

Enterprise Edge provides detailed performance information for the system and the system resources. The statistics are shown in charts or table format. If a performance display is active, it is automatically updated with real-time performance information in time increments that you set.

Note: The statistics generating puts an important workload on the Enterprise Edge server CPU, connecting network, and web client. Exercise caution when running statistics.

Generating System Performance Statistics

Enterprise Edge provides statistical information on system throughput and other performance-related information.

System performance information includes:

- System CPU Usage (graph or table format)
- Memory Usage (graph or table format).

To generate system performance statistics,

1. From the navigation tree, click **System**.
   The **Performance** menu is enabled.

2. From the **Performance** menu select the statistical information you want the system to generate, in the format of your choice.
   The chart of table appears.

3. From the **Counter Type** list, select the type of information you want the system to generate.

4. From the **Polling Interval**, select at which interval you want the system to collect the information.

Error Messages

Enterprise Edge displays error messages when system or processing errors occur. Error message are made of two parts: the error string and the error number.

The error string includes the error description and the context of the error.

The error number is a three-part number that uniquely identifies the error. Be sure to note the error number when communicating with TSC to resolve the problem.

User Actions

Some Enterprise Edge errors are caused by a wrong parameter value. For these errors, the recommended action resolves the problem. Other possible errors are caused by an internal transition of states that puts the system and the user in an error condition. In this event, assistance from TSC is required to resolve the problem.

Note: Any Enterprise Edge errors that are not listed in this manual are advanced and require assistance from TSC for resolution.

Errors List

In the following list, in cases where multiple errors can happen in a particular context, a wild-card representation is used.

Error Number	Description	Action
2.5.4	This is an invalid data error. There was an error in setting system date. Reason: The date, month or year component contains a zero or negative value.	Provide the correct date value.
2.xx.4	These are various errors related to an error in setting system date Reason: The system rejected the date for various reasons. The reasons could be that it is beyond the range of dates supported. For example, 01/01/0001 is invalid date	Make sure system settings are valid.
2.5.6	This is an invalid data error. There was an error in setting system time. Reason: The hour or minute component contains a negative value.	Provide the correct date value.
2.xx.6	These are various errors related to an error in setting system time	Correct the error in the time format.
2.5.8	This is an invalid data error. There was an error in setting system name. Reason: The system name does not follow the standard conventions.	Make sure that your system name does not contain any special characters (hyphens are allowed, in addition to letters and digits), and that it does not exceed 15 characters in length.

5.4.59	This is an invalid configuration error. There was an error getting or setting DHCP parameters. Reason: You were adding an IP Address Range and/or Excluded Address Range and the first field you entered had a wrong key value. In the dialog boxes that appear to add the entries, the first field is a key that should match certain naming conventions. The conventions are given the label to those fields.	Follow the conventions given on the dialog boxes. For IP Address Ranges, use keys like 'Rxx' and for Excluded Address Ranges, use keys like 'Exx'
5.5.39	This is an invalid data value. There are invalid values for the new excluded address range. Reason: The IP Address values specified for the range are not correct. At present, each component in IP address specified in dotted format should be in the range 0-255, not including the boundary values.	Fix the value. If your IP Address range contains more than 255 addresses in it and you need to exclude a range that ends with 255 or starts with. 0, use the next upper or lower value to avoid specifying this value.
5.5.40	This is an invalid data value. There are missing values in the new excluded address range. Reason: Data for each excluded address entry should include two values - one for the start and the other for end. This error happens if one of them is missing.	Enter the missing value and click 'Save' again
5.5.41	This is an invalid data value. The new excluded address range is not completely within an IP Address range. Reason: Excluded Address ranges should be completely contained within a single IP Address range specified for the scope. If a DHCP scope contains more than one IP Address range, then the excluded address ranges specified, if any, may not span outside a single IP Address range in any way. This includes overhanging outside of a single IP Address Range or spanning over multiple IP Address Range.	Fix the over-hanging problem. If required, specify multiple excluded address range. Note: As a guideline, use only one IP Address range, and specify multiple excluded ranges to exclude disjoint parts of it.
5.5.45	This is an invalid data value. The new range overlaps with an existing range Reason: This error happens if the specified excluded range overlaps with another excluded address range or with an address that is already assigned to a DHCP Client computer.	Modify the new excluded address range so that it does not overlap with another or does not include assigned IP addresses. You may also go to the client system that go the assigned address and release IP address before setting the excluded range.

5.16.68	This is an invalid operation. You can't delete the last IP Address range in the scope. Reason: The scope contains only one IP Address range and you are attempting to delete it. You must have at least one IP Address range in the scope all the time. You may modify the last entry, however.	Don't delete the last DHCP range. If you need to change it, modify it. If you don't want the DHCP scope to be operational, change its status to 'Disabled'. If don't want any scope operational, set the status of the DHCP Service to 'Disabled'.
8.4.2.	This is an invalid configuration parameter. There was an error in setting data. Reason: You tried to add a port range or filter and the key field didn't contain the characteristic prefix.	If you are adding a new port-range, make sure the 'PortRange (R#)' field is like 'Rxx' where 'xx' is a number. If you are adding a new filter, make sure that 'Filter (F#)' field looks like 'Fxx' where 'xx' is a number.
8.5.3	This is an invalid data value. There was an error in setting port range Reason: You are setting a port range value and the upper and lower limits are not correct or missing.	Each range should begin with a positive even number and must end with a number greater than the beginning number and must be an odd number. Further, the range values should be less than 65535 (64K)
8.8.3	This is an error in data size. There was an error in setting port range. Reason: You are setting a port range that is too big. At present, only 256 ports can be set in the port-range table.	Consult chapter 3 for a discussion on port ranges in QoS. You may not need that big a range. Reduce it to be under 256 ports in the range.
9.4.2	This is an invalid configuration parameter. There was an error in setting data. Reason: This error can happen when you are setting a community string entry, manager entry or a trap community entry. Each entry uses a characteristic key string as its field name. Use 'Cxx' for community strings, 'Mxx' for manager entries and 'Txx' for trap community entries.	Use appropriate key strings in the dialog boxes, as suggested in their labels.
9.6.4 9.6.5 9.6.6	The object was not found. There was an error in setting <object Name> Reason: This error can happen while setting a community string entry, manager address or trap community entry. Each entry takes a characteristic key field as the first field that should follow certain conventions, and a unique number within the class. If that unique number is 0 or less, this error happens.	Specify correct number for the key field name.

10.5.2	This is an invalid data value for requested data. Reason: This can happen happens when user enters values into a dialog box and clicks 'Save' on it. If any of the fields had some strict format specified for it (say dotted format for an IP address) and if you entered a wrong value, it would beep when you tab out of the field. If you ignored that beep, the GUI would reject the field and when you clicked 'Save' it didn't send the field to the Enterprise Edge system, there by causing this problem.	Follow the rules precisely. If the IP address has only 1 digit, add zeros in order to make them 3-digit in each segments of the dotted notation. For example 000.000.001. Make sure to scroll to the bottom of the screen to add all required values.
11.5.2	This is an invalid data value for password. Reason: The user was changing a user profile and the password entered in 'password' and 'confirm password' fields do not match.	Match the passwords.
11.19.9	Failed to Delete. Required at least one user with read-write privilege. Reason: You are attempting to delete the last existing user with READ-WRITE privilege. This operation is not permitted, as it would not allow you to make any other changes to user configuration or other system configuration.	Add another user with read-write privilege before deleting the concerned user id.
11.12.10	Failed to Update. Required at least one user with read-write privilege. Reason: You are attempting to modify the last existing user with READ-WRITE privilege. At this time, no modifications are permitted to the last READ-WRITE user.	Add another user with READ-WRITE privilege before modifying the concerned user id.
14.4.21	Invalid Configuration Parameter. Error in setting interface parameter Reason: You're setting a static route, input filter or output filter under an interface and you didn't enter a correct characteristic key field in the dialog box. Values for these fields should strictly follow the convention provided in the labels for them. It should be something like 'SRxx' for static routes, 'IFxx' for input filters and 'OFxx' for output filters.	Make sure your key names are as per convention and provide unique values for the number component.

14.17.40 14.17.41	Command failed. Error in setting action for input/output filters Reason: You were attempting to set the action for input/output filters on the interface. The operation failed because, there were no input or output filters defined for the interface.	Add an input or output filter before setting the action
14.17.68	Command failed. Error is setting static route. This problem is caused by a mismatch in destination network address in its subnet mask specified in the route.	Match them. Bitwise 'AND' of destination address and subnet mask should be equal to the destination address.
	The routing protocol is changed and the screen didn't update.	Refresh the screen by clicking on 'View Refresh' menu item.
	The routing protocol for the interface shows up as 'RIP'. But no RIP configuration parameters show up on the screen	Set the routing protocol back to 'NONE' and then set to 'RIP' again. The RIP configuration field would show up.
14.5.77	Invalid Data Value. Static default route is not permitted in this version. Reason: You were setting a static route that was a default route for the system. In this release of Enterprise Edge, setting default routes as static routes is not permitted. The default route is managed by the 'Net Link Manager' component that accepts the address of next hop router on the primary and then adds or deletes (manages) the default route in the system.	None

MIB II Information

Here is the mapping between Enterprise Edge counters shown in statistics windows and standard MIB-II variables where applicable.

This section includes:

- Counters Shown at LAN and WAN Interface Levels
- Counters Shown at LAN and WAN Interface Levels
- ICMP Counters
- UDP Counters
- TCP Counters
- QoS Session Counters
- QoS Best Effort Traffic Counters
- QoS Dropped Packets Counters
- QoS Graph Counters

- QoS Best Effort Queue Counters

Counters Shown at LAN and WAN Interface Levels

1. Byte Received:	ifInOctets
2. Byte Sent:	ifOutOctets
3. Byte Total:	no equivalent (ifInOctets and ifOutOctets)
4. Current Bandwidth:	ifSpeed
5. Output Queue Length:	ifOutQLen
6. Packets Outbound Discarded:	ifOutDiscards
7. Packets Outbound Errors:	ifOutErrors
8. Packets Received Discarded:	ifInDiscards
9. Packets Received Errors:	ifInErrors
10. Packets Received Non-Unicast:	ifInNUcastPkts
11. Packets Received Unicast:	ifInUcastPkts
12. Packets Received Unknown:	ifInUnknownProtos
13. Packets Received:	no equivalent
14. Packets Sent Non-Unicast:	ifOutNUcastPkts
15. Packets Sent Unicast:	ifOutUcastPkts
16. Packets Sent:	no equivalent
17. Packets:	no equivalent

ICMP Counters

Note: Shown on the **Performance** menu under **Resources** heading.

1. Messages Outbound Errors:	icmpOutErrors
2. Messages Received Errors:	icmpInErrors
3. Messages Received:	icmpInMsgs
4. Messages Sent:	icmpOutMsgs
5. Messages:	no equivalent (icmpInMsgs + icmpOutMsgs)
6. Received Address Mask:	icmpInAddrMasks
7. Received Address Mask Reply:	icmpInAddrMaskReps
8. Received Destination Unreachable:	icmpInDestUnreachs
9. Received Echo Reply:	icmpInEchoReps
10. Received Echo:	icmpInEchos

11. Received Parameter Problem:	icmpInParmProbs
12. Received Redirect:	icmpInRedirects
13. Received Source Quench:	icmpInSrcQuenchs
14. Received Time Exceeded:	icmpInTimeExcds
15. Received Timestamp Reply:	icmpInTimestampReps
16. Received Timestamp:	icmpInTimestamps
17. Sent Address Mask:	icmpOutAddrMasks
18. Sent Address Mask Reply:	icmpOutAddrMaskReps
19. Sent Destination Unreachable:	icmpOutDestUnreachs
20. Sent Echo Reply:	icmpOutEchoReps
21. Sent Echo:	icmpOutEchos
22. Sent Parameter Problem:	icmpOutParmProbs
23. Sent Redirect:	icmpOutRedirects
24. Sent Source Quench:	icmpOutSrcQuenchs
25. Sent Time Exceeded:	icmpOutTimeExcds
26. Sent Timestamp Reply:	icmpOutTimestampReps
27. Sent Timestamp:	icmpOutTimestamps

UDP Counters

1. Datagrams No Port:	udpNoPorts
2. Datagrams Received Errors:	udpInErrors
3. Datagrams Received:	udpInDatagrams
4. Datagrams Sent:	udpOutDatagrams
5. Datagrams:	no equivalent (udpInDatagrams + udpOutDataGrams)

TCP Counters

1. Connection Failures:	tcpAttemptFails
2. Connections Active:	tcpActiveOpens
3. Connections Established:	tcpCurrEstab
4. Connections Passive:	tcpPassiveOpens
5. Connections Reset:	tcpEstabResets
6. Segments Received:	tcpInSegs

7. Segments Retransmitted: tcpRetransSegs

8. Segments Sent: tcpOutSegs

9. Segments: no equivalent (tcpInSegs + tcpOutSegs)

QoS Session Counters

Note: These are proprietary counters implemented by QoS Provider Module.

1. Not Served Priority Sessions: The number of premium priority sessions declined by the QoS module - probably due to bandwidth restrictions.

2. Requested Priority Sessions: Total number of premium priority sessions requested

3. Served Priority Sessions: Number of premium priority sessions admitted.

QoS Best Effort Traffic Counters

Note: This is a proprietary counter.

1. Total Best-Effort Octets: Total number octets carried in best-effort level

2. Total Best-Effort Packets: Total number of packets carried in best-effort level.

QoS Dropped Packets Counters

Note: Proprietary counter in QoS.

1. Total Dropped Octets: Total number of octets dropped, probably due to insufficient buffer.

2. Total Dropped Packets: Total number of dropped packets.

QoS Graph Counters

1. Total Octets: Total number of octets sent by QoS

2. Total Packets: Total number of packets sent by QoS

3. Total Priority Octets: Total number of octets carried in premium priority.

QoS Best Effort Queue Counters

Note: This is a proprietary counter.

1. Total Queue XX Octets: Total number of octets carried at specified queue's priority.

2. Total Queue XX Packets: Total number of packets carried at specified queue's priority.

3. Total Queue XX Packets Dropped: Total number of packets dropped at specified queue - probably due to insufficient buffer space.

Maintenance programming for telephony resources

When you perform maintenance on your Enterprise Edge system, you must know the system version and the status of each of your Media Bay Modules. For procedures on how to access this information, refer to the following:

- System version on page 278
- Media Bay Module status on page 279

For information on the logs generated by your Enterprise Edge system, refer to:

- System test log on page 282
- System administration log on page 283
- Network event log on page 284

For information on alarm codes and event messages, refer to Alarm codes on page 285 and Event messages on page 285.

If you want to run a line loopback, payload loopback, card loopback or continuity loopback test, refer to Tests on page 294.

For information on system statistics and metrics, refer to:

- CSU statistics on page 297
- Link Status on page 301
- Metrics on page 301

For information on physically moving an existing telephone, refer to Moving telephones on page 302.

System version

System version allows you to check the version number of the System Processor (SP) software, that resides on the Media Services Card (MSC).

1. Choose **Resources** and click on the **Media Services Card** heading.
   The version number of the software appears in the **Version** box.

2. Write the version number on the appropriate Maintenance record.

   Note: You can use the version number to determine the software release and it may be required by support staff if a software fault occurs.

Media Bay Module status

Media Bay Modules selection allows you to view the status of all the modules as well as identify any device or lines connected to the system. This allows you to isolate any malfunctioning part of the system. In addition, you can use the **Media Bay Module** selection to disable and enable modules and devices. For more information, refer to one of the following procedures.

- Display the Media Bay Module status on page 279
- Disable a module on page 279
- Enable a module on page 280
- Identify a device connected to the system on page 280
- Disable a device on page 281
- Enable a device on page 281

Display the Media Bay Module status

Use this procedure to display module type, the number of sets connected to the module, the number of busy sets and the module's state:

1. Choose **Resources**, **Media Bay Modules**.
   The window displays **Bus 02** through to **08**.

2. Click on the Bus you want to view. For example, **Bus 02**.
   The **Configuration** menu is enabled and the status information of the module associated with that bus appears.

Disable a module

You must disable a module before you replace it. In addition, you may be able to clear a hung line by disabling and enabling the affected module.

Use Page feature, on your system, prior to disabling.
Use the Page feature to inform users that you are about to disable a module. Indicate that they may experience delays in the performance of their devices.

1. Choose **Resources**, **Media Bay Modules** and click on the **Bus ##** you want to disable.
   The **State** box indicates that the module is enabled. The **Configuration** menu option is enabled.

2. On the **Configuration** menu click **Disable**.
   The system displays a warning that this action will disable the entire module and all of its devices.

3. Click **OK**. The system disables the module in one minute (or immediately, if the status is idle). Click **Cancel** to leave this display without disabling the module.

Enable a module

Use the following procedure to enable a disabled module.

1. Choose **Resources**., **Media Bay Modules** and click on the **Bus** associated with the module you wish to enable.
   The **State** box indicates that the module is disabled and the **Configuration** menu is enabled.

2. On the **Configuration** menu click **Enable**.
   The system displays a message indicating that the module is being enabled.

Identify a device connected to the system

You may wish to check a device's version number for compatibility with the system. Use the following procedure to display status information for any device connected to the system.

1. Choose **Resources**, **Media Bay Modules**, **Bus ##**, **Port #**, **Channels**.

2. Click on the **B1** heading to display the device connected to the B1 channel or click **B2** to display the device connected to the B2 channel.
   The window displays the device, its type, the version number of the device and its state.

3. If there is an add-on device attached to the telephone such as a central answering position module or a Busy Lamp Field, expand the **B1** or **B2** heading and click on the **Addons** heading to display the add-on device.

The following table lists some of the device types that may appear on the Enterprise Edge device identification display.

Display	Explanation
M7100	M7100 telephone
M7310	M7310 telephone
M7324	M7324 telephone
1: CAP1	First CAP module attached to an M7324 telephone
2: CAP2	Second CAP module attached to an M7324 telephone
Nortel Networks ATA 2	Analog Terminal Adapter

Disable a device

Give notice that you are disabling equipment.
Inform people that you are going to disable their devices.

Pick a suitable time to disable devices. Disabling a port will disconnect users from their calls.
Do not disable devices when many people are using the Enterprise Edge system. Wait until after regular office hours.

Do not enable or disable ports during the first two minutes after plugging in your system.
If you enable or disable ports in the first two minutes after powering up, incorrect ports may be enabled or disabled. To recover from this, disable, then enable the affected modules using the **Media Bay Modules** selection.

Use the following procedure to disable a device immediately.

1. Identify the device you wish to disable. For information on how to perform this procedure, refer to Identify a device connected to the system on page 280.

2. On the **Configuration** menu click **Disable**.
   The system displays a warning that this action will disable the port.

3. Click **OK**.
   The system disables the device in one minute (or immediately, if the device is idle). Press **Cancel** to leave this display without disabling the device.

Enable a device

Use the following procedure to enable a disabled device:

1. Identify the device you wish to disable. For information on how to perform this procedure, refer to Identify a device connected to the system on page 280.

2. Click on the device you want to enable.

3. On the **Configuration** menu click **Enable**.
   The system displays a message indicating that the device is being enabled.

System test log

The System test log shows you a list of diagnostic test results, audits, event messages, and alarm codes. By using this feature you can check log items, any current alarms, timing of log events and the number of consecutive occurrences of an event or an alarm. In addition, you can use the **System test log** selection to erase the log.

The System test log holds a maximum of 20 items. You should check and record these items at regular intervals. Erase the log after dealing with all the items.

Use the **System test log** selection under **Diagnostics**, **MSC** to perform one of the following procedures.

- Display information on the items in the System test log on page 282
- Erase the log on page 282

Display information on the items in the System test log

You can display information on any item in the System administration log using the following procedure.

1. Choose **Diagnostics**, **MSC**, **System test log**.

2. Double click on the **System test log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3. Click on an item. Information about the log item appears.
   The description attribute indicates if the item is an event or alarm and includes the associated code. The severity, repeats, time and parameters of the event or alarm appears. For more information on the event or alarm, refer to Alarm codes on page 285 or Event messages on page 285.

   Note: Alarms also appear in the Windows NT event log.

4. Write down the item on the System administration log record and repeat these steps until you record all the items.

Erase the log

You can erase log items from the System Test log using the following procedure.

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Diagnostics**, **MSC**, and click on the **System test log** heading.

2. Click **Del All** from the menu above the navigation tree.
   The system displays a message asking you to confirm that you wish to remove all of the items.

3. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

System administration log

The System administration log keeps a record of administrative events such as sessions in which a change was made, invalid password attempts, and password changes. You can check the items in the log, check when each item in the log occurred and you can erase the log.

Note: The System administration log holds a maximum of ten items. Erase the log after dealing with all the items.

Use the **System admin log** selection under **Diagnostics, MSC** to perform one of the following procedures.

- Display information on the items in the System Administration log on page 283
- Erase the log on page 283

Display information on the items in the System Administration log

You can display information on any item in the System administration log using the following procedure.

1. Choose **Diagnostics**, **MSC**, **System admin log**.

2. Double click on the **System admin log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3. Click an item.
   Information about the log item appears. The description attribute indicates if the item is an event or alarm and includes the associated code. The severity, repeats, time and parameters of the event or alarm appears. For more information on the event or alarm, refer to Alarm codes on page 285 or Event messages on page 285.

   Note: Alarms also appear in the Windows NT event log.

4. Write down the item on the System administration log record and repeat these steps until you record all the items.

Erase the log

You can erase log items from the System Administration log using the following procedure.

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Diagnostics**, **MSC**, **System admin log**.

2. Double click on the **System admin log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3. Click **Del All** from the menu above the navigation tree.
   The system displays a message indicating that this will remove all of the items.

4. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

Network event log

The Network event log keeps a record of events and alarms that are specific to the T1 network interface. You can check the items in the log, check when each item in the log occurred and you can erase the log.

The Network event log holds a maximum of twenty items. Erase the log after dealing with all the items.

Use the **Network event log** selection under **Diagnostics, MSC** to perform one of the following procedures.

- Displaying information on the items in the Network event log on page 284
- Erase the log on page 285

Displaying information on the items in the Network event log

You can display information on any item in the Network event log using the following procedure.

1. Choose **Diagnostics, MSC**.

2. Double click on the **System test log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3. Click an item. Information about the log item appears.
   The description attribute indicates if the item is an event or alarm and includes the associated code. The severity, repeats, time and parameters of the event or alarm appears. For more information on the event or alarm, refer to Alarm codes on page 285 or Event messages on page 285.

   Note: Alarms also appear in the Windows NT event log.

4. Write down the item on the System administration log record and repeat these steps until you have recorded all the items.

Erase the log

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Diagnostics, MSC**, **Network event log**.

2. Double click on the **System test log** heading to display all the items in the log. If there are no log entries, the navigation tree indicates that there are no subheadings.

3. Click **Del All** from the menu above the navigation tree.
The system displays a message indicating that this will remove all of the items.

4. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

Alarm codes

The Enterprise Edge system generates alarm codes after system disconnections or after certain anomalies in system operation. All alarm codes appear at the Alarm telephone, in the System test log of a Maintenance session and in the Win NT event log. For a more complete description of alarm and event codes consult your technical support representative.

Tips

You can assign the Alarm telephone in Feature settings under System programming.

Alarms have a higher severity than events. Attend to alarm codes before event messages.

Alarm code information that is specific to Companion components is included in the.

An alarm code may not appear until two minutes after it is triggered. If the system is powered off when the alarm is triggered, the alarm code does not appear until two minutes after the system is powered on.

Event messages

Event messages appear as items in the System administration log or the System test log of the Maintenance session. Most of these event messages can only be caused by an unusual combination of events, and should rarely occur.

Each event has a severity number. An “S” preceding this number, “S4” for example, may appear in the event message. “S9” is the most severe. If the log is full, new event messages with a higher severity number replace existing event messages of a lower severity. For this reason, you should check event messages at regular intervals. You can then deal with all messages before they are replaced. The time that the message is recorded is also provided.

Event message information that is specific to Companion components is included in the Companion event messages (North American systems only) on page 291.

For every event message that you see:

1. Refer to Significant event messages on page 286.

2. Determine if the event caused the system to automatically restart. For more information, refer to the table on Event Message on page 289.

Significant event messages

The following table lists event messages that are relevant to maintenance activities.

Event message	The event message is recorded when…
Evt:210-YYYZ S4	Loopback test YYY on Trunk module Z has been started
Evt:211-YYYZ S4	Loopback test YYY on Trunk module Z has been stopped
Evt:220-3546 S4	the Sys admin log has been cleared by the DN (3546 in this case)
Evt:221-3546 S4	the Sys test log has been cleared by the DN (3546 in this case)
Evt:222-3546 S5	the DN (3546 in this case) enters the debugging facility that is password protected
Evt:255 S9	administered mode is not supported by the module plugged into the slot
Evt:260-0302 S8	the system takes the access line on port 0302 out of service because no current was detected
Evt:261-0302 S1	the access line on port 0302 is returned to service after current was detected (see Evt:260)
Evt:268-07 S8	Dialing filter 07 has lost data due to a fault in the system memory
Evt:269-3546 S8	the Line/set filter for the DN (3546 in this case) has lost data due to a fault in the system memory
Evt:299 S1	the system powers up after a power failure
Evt:327 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:328 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:329 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:330 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:336 S5	long term alarm has been surpassed in the EE-DTM
Evt:373 S5	the system restart diagnostic tool has been activated
Evt:407 S2	there are no more codes for Speed Dial numbers
Evt:408 S2	there is no more memory for Speed Dial codes

Event message	The event message is recorded when…
Evt:415-3546 S3	an invalid customer password has been entered by the DN (3546 in this case)
Evt:418 S7	a DN change is successful
Evt:419 S2	the time setting has been changed
Evt:421 S8	a DN change failed
Evt:422-3546 S6	a length change by the DN (3546 in this case) has been requested
Evt:423-3546 S6	an individual DN change has been requested by the DN (3546 in this case)
Evt:441 S2	a timeout occurred while waiting for ANI or DNIS digits to be received
Evt:442 S5	a timeout occurred while waiting for ANI or DNIS digits to be received
Evt:454 S5	Invalid password entered
Evt:458 S4	Call-by-Call NVRAM data is corrupt and all the values have been reset to default.
Evt:459 S9	DN length has been changed to less than 3 digits
Evt:680 S9	wireless system is disabled
Evt:681 S9	activation or recovery code entered
Evt:683 S9	new base station configuration detected
Evt:687 S4	the data driver has received a bad call reference
Evt:688 S4	the data driver has received a bad data event
Evt:689 S4	the data driver could not allocate a new index
Evt:690 S4	no response to the system within 10 seconds of being sent an initialization message
Evt:691 S4	no response to the system within 3 seconds
Evt:692 S4	a bad parameter value has been received in a stimulus message from the data device
Evt:693 S3	old data to be discarded has been detected
Evt:694 S4	RADAR flow control has received a bad stimulus message from an off-core application
Evt:695 S4	attached set denied request for a B-channel
Evt:696 S2	corrupt CLID length
Evt:697 S2	an asynchronous data report generated by SDI
Evt:698 S8	incorrect software key entered
Evt:799 S7	a call processing error has occurred on an ISDN line
Evt:822 S8	Alarm code 63 is sent because there are no DTMF receivers for an incoming call
Evt:882 S9	mobility data re-evaluation sequence initiated
Evt:883 S4	an invalid dial pulse signal was received by the EE-DTM
Evt:992 S6	auto attendant error

How to read an event message

In the event message shown below, Evt799 indicates a call processing error has occurred on an ISDN line.

Evt799-031 02S7

The event number Evt799 is followed by a number representing the line or loop number, and a code for the type of error. In this example, the error has occurred on line 031 and the error code is 02.

The following table lists some of the error codes and their meanings.

Error code	Meaning
01	Internal software error. Cannot acquire the B-channel from the B-channel arbitrator.
02	Internal software error. There is no free line available for the call.
03	A call that is not on the B-channel has been attempted. These kind of calls are part of EKTS service, which is not supported by this version of the software. Check with your service provider to make sure your package does not include EKTS service.
04	Internal software error. Failed to instantiate on the chain.
05	Internal software error. Activation procedure failed.
06	Internal software error. Index conversion failed.
07	Unexpected digits on a Manual answer mode line. Configuration of the system and the network connection may not match.
09	Cannot get vterm (virtual terminal) from the Vterm Server.
0C	Internal software error. Already instantiated on the chain.

Events that cause a system restart

You should rarely see any event messages that are not described in the Significant event messages on page 286. If you do see one of these event messages, the system has followed its normal recovery from an unusual combination of system events. Although the problem is not a serious one, you should report repeated occurrences of the event number as soon as possible.

As a result of some events, the system automatically restarts itself. The table on the next two pages lists all the event numbers and identifies the events associated with system restarts.

Most of these events are recorded in the **System test log**. The few exceptions to this are recorded in the **System administration log**, as indicated.

Event Message	System Restart	Event Message	System Restart
101-106	Yes	400 (Admin log)	Yes
107	No	401-403	No
108-112	Yes	405-411	No
113	No	412-419 (Admin log)	No
114-116	Yes	421-423 (Admin log)	No
117	No	424-425	No
118-120	Yes	426-430	Yes
121-123	No	431	No
124-125	Yes	432	Yes
126-129	No	433	No
130	Yes	441-442	No
131-132	No	453	No
133-134	Yes	454	No
135-136	No	458-459	No
137	Yes	600-602	Yes
138-150	No	603-613	No
151	Yes	614	Yes
152	No	615-629	No
160-164	No	630	Yes
170-173	No	631-646	No
200-211	No	680	No
220 (Admin log)	No	681	No
221-222	No	683	No
223 (Admin log)	No	689-698	No
224	Yes	799	No
225-228	No	800-802	No
229 (Admin log)	No	803	Yes
230-235	No	804-807	No
245-248	Yes	808	Yes
250-256	No	809	No

Event Message	System Restart	Event Message	System Restart
260-271	Yes	810	Yes
280-283	No	811-820	No
285-298	Yes	823	Yes
299	No	824-825	No
327	No	851	No
328	No	882	No
329	No	883	No
330	No	900	No
336	No	940-943	No
373	No	950-989	No

Companion event messages (North American systems only)

Table 1 Event messages

Event message display		Cause
Evt:275-3546	S8	(U.S. only) Unable to activate all registered portables. The system ran out of portable credits. One event is generated per portable that failed to activate. The repetition of the corresponding alarm code 59 indicates how many additional credits must be purchased.
Evt:301-1031	S5	The Base Station (on port 0103 in this case) cannot successfully receive the data image. Both radios belonging to the Base Station are disabled. This may occur if the flash EEPROM is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:302-1031	S5	The Base Station (on port 0103 in this case) cannot be written to during data transfer. Both radios belonging to the Base Station are disabled. The Base Station's flash EEPROM is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:303-1031	5	The Base Station (on port 0103 in this case) cannot be synchronized with the other Base Stations in the system. Both radios belonging to the Base Station are disabled. The Base Station hardware is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:304-1032		A B2 channel radio (radio 2 on port 0103 in this case) cannot be synchronized with other radios because of system overload.
Evt:305-01032	S5	A B2 channel radio (radio 2 on port 0103 in this case) cannot be synchronized because the B1 radio was disabled in maintenance. Both radios belonging to the Base Station (on port 0103 in this case) are disabled. The B1 radio must be operational to synchronize both radios of the Base Station with other radios in the system. Two events are raised: one for the B1 channel radio and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:306-01031	S5	A radio (0103-1 in this case) cannot be synchronized because there are no B2 channel radios. Both radios belonging to the Base Station (on port 0103 in this case) are disabled.Two events are raised: one for the B1 channel radio in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:307-0109100	S5	A recoverable RIM fault has occurred The RIM is reset. If a link is active when this error occurs, the link is dropped. The radio (0109-1 in this case) is returned to service.

Event message display		Cause
Evt:307-0109101	S5	An unrecoverable RIM fault has occurred The radio (0109-1 in this case) is disabled and taken out of service. If a link is active when this error occurs, the link is dropped. A corresponding alarm code 53 occurs.
Evt:307-0109102	S5	The built-in self-test on the Base Station has failed The radio (0109-1 in this case) is disabled and taken out of service. If a link is active when this error occurs, the link is dropped. A corresponding alarm code 53 occurs.
Evt:308-0103	S5	The Base Station is connected to a system that supports a radio protocol that the Enterprise Edge does not understand.
Evt:664	S8	There is a bad signature.
Evt:665	S4	(U.S. only) there are insufficient radio credits.
Evt:666	S5	(U.S. only) radio credits decreased.
Evt:667	S5	(U.S. only) UTAM keys are required.
Evt:668	S5	(U.S. only) UTAM test failed.
Evt:669	S5	Evaluation override is finished.
Evt:670	S5	Disablement test is active.
Evt:671	S5	Disablement test is finished.
Evt:672	S5	System initialization is beginning.
Evt:673	S5	System initialization is finished.
Evt:675	S5	Demo system.
Evt:831	S5	Software error dealing with Base Station.
Evt:832	S5	System problem with locating portable telephones.
Evt:833	S5	The radio driver software which directly controls the Base Stations' device has experienced an internal error.
Evt:834	S5	System problem with locating portable telephones.
Evt:835	S5	Wireless system access error.
Evt:836	S5	Wireless system access error.
Evt:837	S5	Trying to register an incompatible wireless device.
Evt:840	S5	Wireless system software error in dealing with a portable telephone.
Evt:841	S5	Wireless system software error.
Evt:842	S5	Portable does not support specific display character.
Evt:843	S5	Internal radio driver error.
Evt:848	S5	A cell manager has been unable to register with the router.
Evt:849	S5	Synchronization error.
Evt:850	S5	Synchronization error.
Evt:851	S5	Base Station software error.
Evt:852	S5	The Data Transfer server has been told by the Base Station that an error has occurred.
Evt:853	S5	The Data Transfer server has been told by the Base Station that an error has occurred.

Event message display		Cause
Evt:854	S5	Invalid event for Data Transfer.
Evt:855	S5	Internal wireless subsystem software error.
Evt:856	S5	Internal wireless subsystem locator error.
Evt:859	S5	All possible wireless telephone numbers have been registered to portable telephones. No directory number is available to handle the registration Link setup request.
Evt:864	S5	A Base Station has received a corrupted stimulus message.
Evt:865	S5	The Base Station does not understand the received stimulus message. This occurs when you are trying to use a type of portable that the system does not support.
Evt:869	S5	Wireless subsystem language loading error.
Evt:870	S5	Firmware downloading to Base Station.
Evt:871	S5	Basestation download is complete.
Evt:872	S5	Wireless subsystem error.
Evt:873	S5	Wireless subsystem Common Signaling Channel server software error.
Evt:877	S5	Wireless auto-admin (Re-Eval) subsystem detected that a data re-evaluation is required.
Evt:878	S5	Wireless data re-evaluation has started.
Evt:879	S5	Wireless data re-evaluation has completed.
Evt:881	S5	Wireless auto-admin (Re-Eval) indicating that a configured cell failed to come on-line. Alarm 23 displays cell that failed.
Evt:884	S5	The Wireless auto-admin (Re-Eval) subsystem has detected an error.
Evt:885	S5	Sequencer functionality has detected an error.
Evt:886	S5	The Wireless auto-admin (Re-Eval) Initial Intelligence component has detected an error.
Evt:887	S5	The Wireless auto-admin (Re-Eval) radio Sniffing component has detected an error.
Evt:888	S5	The Wireless auto-admin (Re-Eval) Radio Manager has detected an error.

Note: Companion alarm codes appear in the Windows NT™ event log.

Tests

Enterprise Edge allows you to run tests to verify the integrity of the installation wiring for the telephone sets. Before you run any tests, use the procedure, DN-to-port conversion on page 296, to determine the port associated with a particular DN.

Choose an appropriate time to run tests.
A good time to run tests is after office hours.

The following messages may appear on the Alarm Telephone during Loopback tests.

Message	Explanation
EVT: 210-YYYZ	Loopback test YYY on Trunk module Z has started
EVT: 211-YYYZ	Loopback test YYY on Trunk module Z has ended

You can start and stop Loopback tests under the **Diagnostics** heading. Run only one test at a time on an EE-DTM. You can move on to another programming task while the loopback test is running. While the loopback test is running, the green “in Service” LED on the EE-DTM flashes.

If you administer the internal CSU on a line loopback and payload loopback, then the central office can also invoke and stop tests. In order to be able to run a payload loopback test, you must configure the EE-DTM for extended superframe format.

The Enterprise Edge system allows you to run the following tests:

- Line loopback test on page 294
- Payload loopback test on page 295
- Card loopback test on page 295
- Continuity loopback test on page 295

Use the procedure, Start a loopback test on page 296, to run any of these tests.

Line loopback test

The line loopback test loops the full 1.544 Mbps signal received from the network back to the network. The looped signal regenerates without any change in the framing format and without the removal of any bipolar violations. The line loopback test can also be invoked and stopped remotely using the in-band signal or via the facility data link (FDL) in extended super frame (ESF) format.

The line loopback test must be run in coordination with the T1 or PRI service provider. Some test patterns can cause the EE-DTM to reset. To avoid this, start the line loopback test from your system before the T1 or PRI service provider begins their test, and stop the line loopback test from your system after the T1 or PRI service provider ends their test.

Payload loopback test

The payload loopback test loops the received information bits (192 per frame) back to the network. You can also remotely invoke and stop the payload loopback test through the facility data link (FDL) in extended super frame (ESF) format.

The payload loopback test must be run in coordination with the T1 service provider. Some test patterns can cause the EE-DTM to reset. To avoid this, start the payload loopback test from your system before the T1 service provider begins their test, and stop the payload loopback test from your system after the T1 service provider ends their test.

Card loopback test

The card edge loopback test loops the outgoing signal on the EE-DTM back to its internal received signal path. The system disconnects signal paths to the external network.

Continuity loopback test

The continuity loopback test shorts the tip and ring pair of the receive signal path with the transmit signal path. This test allows you to check the metallic continuity of the external wiring.

Start a loopback test

Give notice that you are running a loopback test.
Calls on all T1 or PRI lines on the EE-DTM will be automatically dropped when a loopback test is invoked. Use the Page feature to notify people using the system that a test is about to begin and that calls will be disconnected.

1. Choose **Diagnostics**, **Trunk Modules**.

2. Double click on the bus that contains the card you want to test. For example, **Bus 02**.

3. Double click on the appropriate module on this bus. For example, **Module 1**.

4. Click on **Loopback Tests**.
   The **Configuration** menu option is enabled. The loopback status box displays the type of test currently running.

   Note: If there is an analog module in the slot or the slot is empty, the box displays **Not equipped**.

5. On the **Configuration** menu click **Start loopback** to begin the test.
   The system displays the Loopback type selection window.

6. From the drop-down menu, select the test you want to run and then click **OK**.
   The options are **Line**, **Payload**, **Card edge** or **Continuity**.

   Note: To end the test at any time, click **Stop loopback** on the **Configuration** menu.

DN-to-port conversion

If you know a telephone's DN, you can determine the port associated with this DN, using the following procedure.

1. Choose **Diagnostics**, **MSC**, and click on the **DN-to-port conversion** heading.

2. Type the DN in the **DN to convert** box and press **Enter**.
   The system displays values in the Device port and Device channel boxes.

Debug

Restart info

To view the Restart info:

1. Choose **Diagnostics**, **MSC**, **Debug**, and click on the **Restart info** heading.
   The **Restart info** summary screen appears.

2. On the **Configuration** menu click **Clear restart info** to clear the log.

Registers

To view the Registers information:

1. Choose **Diagnostics**, **MSC**, **Debug**, **Restart info**.

2. Click on the Registers heading.
   The **Registers** summary screen appears.

Message monitoring

1. Choose **Diagnostics**, **MSC**, **Debug**, and click on the **Message monitoring** heading.
   The **Message monitoring** screen appears.

CSU statistics

Each EE-DTM has an internal channel service unit (CSU). When enabled, the internal CSU monitors the quality of the received T1 signal and provides performance statistics, alarm statistics and diagnostic information.

EE-DTMs must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.

For more information, refer to:

- Statistics collected by the Enterprise Edge system on page 297
- Enable the internal CSU on page 298
- Check the performance statistics on page 299
- Check the CSU alarms on page 299
- Check carrier failure alarms on page 299
- Check bipolar violations on page 300
- Check short term alarms on page 300
- Check Defects on page 300
- Reset all statistics on page 300

Statistics collected by the Enterprise Edge system

The system accumulates three performance parameters:

- errored seconds (ES)
- severely errored seconds (SES)
- unavailable seconds (UAS)

These parameters are defined as per TIA-547A. Errored seconds are enhanced to include control slip (CS) events. Only near-end performance data is recorded.

The internal CSU continuously monitors the received signal and detects four types of transmission defects:

- any active carrier failure alarms (CFA) (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI)
- the number of bipolar violations that occurred in the last minute
- any defects (loss of signal LOS, out of frame OOF, alarm indication signal AIS) that occurred in the last minute
- the number of milliseconds of short term alarms (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI) in the last minute. A short term alarm is declared when the detected defects persist for tens of milliseconds.

A carrier failure alarm (CFA) is a duration of carrier system outage. CFA types reported can be mapped to CFAs defined in TIA-547A and TR62411 as follows:

Enterprise Edge	TIA-547A	TR62411
LOS CFA	Red CFA	Red CFA
OOF CFA	Red CFA	Red CFA
AIS CFA	Red CFA	AIS CFA
RAI CFA	Yellow CFA	Yellow CFA

The criteria for declaring and clearing the alarms is selectable to meet those in TIA-547A or TR64211.

Enable the internal CSU

Use the following procedure to enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

1. Choose **Resources**, **Media Bay Modules**.
   The window displays **Bus 02** through to **08**.

2. Choose the appropriate bus. For example, **Bus 02**.

3. Choose **Modules on Bus**.
   The modules on this bus are displayed.

4. Choose the appropriate module. For example, **Module 1**.

5. Click on the **T1 Parameters** heading.

6. In the **Internal CSU** box, select **On** from the drop-down menu.
   The module is temporarily disabled while the internal CSU is enabled.

Check the performance statistics

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose the appropriate bus that contains the module that you want to check.

3. Choose **Module #**, **CSU statistics**, **Performance statistics**.

4. Click on the **Current interval** heading to display the duration of the current 15 minute interval of the selected card, the number of errored seconds (ES), the number of severely errored seconds (SES) and the number of unavailable time seconds (UAS).

5. Double click on the **15 min intervals** heading to display statistics for 15 minute intervals in the last 24 hours, numbered from the most recent (01) to the oldest (96). Click on the most recent interval. The window shows the start time of the interval.

6. Click on the **24-hour summary** heading for an overall summary of the previous 24 hours.
   The **Number of intervals**, **Errored Seconds**, **Severely Errored Seconds**, **Unavailable Seconds**, appear in the summary.

Check the CSU alarms

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Choose **CSU Statistics**, **Alarm statistics** and click on the **Active alarms** heading.
   The display shows all the active alarms of the types **LOS (loss of signal)**, **OOF** (out of Frame), **RAI** (Remote alarm indicator) or **AIS** (Alarm indication signal). For more information on these types of transmission defects, refer to Statistics collected by the Enterprise Edge system on page 297.

Check carrier failure alarms

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Choose **CSU Statistics**, **Alarm statistics**, **CFA alarms**.
   The display shows **LOS (loss of signal)**, **OOF** (out of Frame), **AIS** (Alarm indication signal), **RAI** (Remote alarm indicator), Short-term alarms and Defects. For more information on these types of transmission defects, refer to Statistics collected by the Enterprise Edge system on page 297.

4. Choose the type of alarm you wish to view. For example, **LOS (Loss Of Signal)**.

5. Click on the **Period #**.
   The display shows the Start time of the period.

Check bipolar violations

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Choose **CSU Statistics** and click on the **Alarm statistics** heading.
   The display shows the number of bipolar violations that occurred in the last minute.

Check short term alarms

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Choose **CSU Statistics**, **Alarm statistics**, and click on the **ShortTerm alarms** heading.
   The display shows the short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute.

Check Defects

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Choose **CSU Statistics**, **Alarm statistics**, and click on the **Defects** heading.
   The display shows the first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported in the last minute.

Reset all statistics

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Click on the **CSU Statistics** heading.

4. On the **Configuration** menu, click **Clear CSU statistics.**
   The system displays a message indicating that this will remove all of the statistics.

5. Select **OK** to erase all the current statistics and begin collecting statistics again.

Link Status

When you purchase PRI from your service provider, you can request the number of B-channels that are allocated for you to use. For example, you may want to use only 12 B-channels instead of 23 B-channels. If this is your situation, you should disable all the B-channels that you do not need.

It is recommended that the number of lines that are deprovisioned on an EE-DTM (configured as PRI) be the same as the number of b-channels that are disabled. For example, If the EE-DTM is on bus 7, when b-channels 13-23 are disabled, you should deprovision lines 73 to 83.

1. Choose **Diagnostics**, **Trunk Modules**.

2. Choose a bus and then choose a module.

3. Choose **B channels**.
   A list of the B channels on this card appears.

4. Click on a channel, for example, **B 01**
   The display shows the status of the PRI channel.

5. On the **Configuration** menu, click **Enable** or **Disable** to change the setting for the channel.

Metrics

The following usage metrics are available with the Enterprise Edge Software:

- CbC limit metrics on page 301
- Hunt Group Metrics on page 302

CbC limit metrics

You can view statistical information on call-by-call limit settings for PRI when the protocol is set to call-by-call routing.

1. Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, **CbC limit metrics**.
   The display shows the pools that supports CbC routing.

2. Choose a pool. For example, **Pool PRI-B**
   The display shows the services in the pool. The services that appear depend upon the PRI protocol.

3. Select a service. For example, **Public**.
   The display shows the settings for the selected service.

To clear the settings for a selected service, click **Clear metrics** on the **Configuration** menu.

Hunt Group Metrics

This feature gives you statistical information on hunt group calls.

1. Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, **Hunt Group Metrics**.
   All the Hunt Groups appear.

2. Click on a **Hunt Group**.
   The display shows all the statistical information for the selected hunt group.

To clear the hunt group metrics, click **Clear group** on the **Configuration** menu.

PSTN fallback metrics

To view the metrics associated with VoIP calls that fallback to the PSTN network.

1. Choose **Diagnostics**, **Service Metrics**, **Telephony Services**, and click on the **PSTN fallback metrics** heading.
   The Last reset time, Fallback requests and Fallback failures values appear.

2. On the **Configuration** menu click **Clear data and time** to reset the metric log.

Moving telephones

You can move a Enterprise Edge telephone to a new location within the system without losing its programmed settings. Set relocation (automatic telephone relocation) must be enabled in system programming. This makes the internal numbers, autodial settings, and personal speed dial codes remain with the telephone when it is unplugged.

Automatic telephone relocation is disabled by default. Use the following procedure to enable set relocation.

1. Choose **Resources**, **Services**, **Telephony Services**, **General settings**, and click on the **Feature settings** heading.

2. In the **Set relocation** box, select **Y** from the pull-down menu.

After set relocation is enabled, unplug the telephone and plug it in again at another location. It may take up to 45 seconds for the system to recognize the telephone.

Tips

All telephones being moved should be relocated before new telephones are plugged into their place. This allows the moved telephones to retain their programmed settings. If a new telephone is plugged into the system before the old telephone is reconnected at a new location, the system will give the old telephone's information to the new telephone, and the old telephone will no longer be recognized by the system.

When changing a telephone's internal number (in programming), wait one minute after Automatic Telephone Relocation.

When you relocate a telephone, the telephone must remain installed and connected in the new location for at least 3 minutes for the programming relocation to be complete. Moving the telephone again before the 3 minute period may result in losing the telephone's programming.

Troubleshooting your Enterprise Edge system

9

These troubleshooting procedures allow you to solve many problems in the Enterprise Edge system. Follow these procedures before replacing any components.

Only qualified persons should service the system.

The installation and service of this unit is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the Enterprise Edge must be connected to an outlet with a third-wire ground.

Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth ground via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (central office lines) removed first.

Under **Diagnostics**, **MSC** there is a **Debug** function which ITAS personnel can use to troubleshoot problems with your Enterprise Edge system. **Debug** is password protected. For more information, contact ITAS.

For more information, refer to the following sections.

- General troubleshooting information on page 305
- Problems with telephones on page 309
- Problems with lines on page 310
- Problems with optional equipment on page 315
- Problems with Trunk or Station Modules on page 320
- Problems for network or remote users on page 321
- Problems with Companion sets (North American systems only) on page 326

General troubleshooting information

- Getting ready on page 306
- Types of problems on page 306
- Basic troubleshooting procedure on page 306

Getting ready

Before you begin troubleshooting, gather all the information that is relevant to your network configuration such as:

- records from people who use the network
- information about other hardware and non-Enterprise Edge features within the public or private network

Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1or PRI service.

Types of problems

The problems you encounter will likely fall into one of the following categories:

Misunderstanding of a feature: A problem may be reported because an Enterprise Edge user is unfamiliar with the operation of a given feature. You may be able to solve the problem simply by demonstrating how to use the feature correctly.

Programming errors: You may encounter problems caused by errors in programming. A feature may have been programmed incorrectly or may not have been programmed at all.

Wiring connections: Wiring problems are caused by loose, unconnected, or incorrect wiring. Use the procedures in the section on checking the hardware as a guide.

Equipment defects: You may encounter problems caused by Enterprise Edge equipment defects. See the appropriate section for problems related to the system hardware.

Basic troubleshooting procedure

Use the following basic troubleshooting procedure as well as the detailed descriptions in this guide. Where more than one procedure is given for a particular problem, the procedures represent different options from which you should select just one.

1. Diagnose the trouble by determining:
    - the types of problems users have experienced
    - the frequency of the problems
    - how many telephones are affected

2. Access the system performance graphs and tables to view the system usage and any system faults. For more information, refer to Viewing system performance and fault alarms on page 307.

3. Check how a feature is being used. A problem may have been reported because of a misunderstanding about how a feature works. Confirm that the person who reported a problem understands the intended use and operation of any feature in question.

4. Run a Station set test (Feature 8 0 5).

5. Check the wiring and hardware connections.

6. If the problem persists, run a Maintenance session as described in Maintenance programming for telephony resources on page 278.

7. If hardware is defective, replace it. If the trouble requires expert advice, use the instructions in How to Get Help on page 307.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Viewing system performance and fault alarms

- System performance graphs and tables on page 308
- Fault Alarm Banner on page 308

System performance graphs and tables

To access the system performance graphs and tables:

1. Choose **System**.

   The Performance, Fault and Tools menu options are enabled.

2. From the **Performance** menu option, select **System CPU Usage Graph**, **System CPU Usage Table**, **Memory Usage Graph** and **Memory Usage Table**.

Fault Alarm Banner

The Alarm Banner provides a window which allows you to continually monitor the Enterprise Edge system for fault alarms. The Alarm Banner is designed to stay on your desktop for quick access. The banner uses a color code to describe the severity of the alarm and provides the number of alarms for each severity level.

To view the system fault alarm banner:

1. From the navigation tree, click **System**.
   The Performance, Fault and Tools menus are enabled.

2. From the **Fault** menu, choose **Fault**.
   The Alarm Banner appears.

3. To view a list of alarms of a particular severity level, click the color coded corresponding box
   or
   click **ALL** (white box) to browse through the complete list of system alarms, regardless of the severity level.

   The Alarm Browser is displayed. See Alarm Browser on page 308 for more information.

Alarm Browser

The Alarm Browser provides detailed description of each alarm occurring within the system. The Alarm Browser contains a Repair Action box which can help you take the correct action to clear an alarm.

To view Alarm Details,

1. From the Alarm Browser screen, click the row corresponding to the alarm for which you want detailed information.
   The row is highlighted.

2. From the Alarm Browser menu, click **Actions** and select **Display Details**.
   The Alarm Details screen appears.

Problems with telephones

For troubleshooting information for your telephone sets, refer to one of the following items:

- Telephone has faulty buttons, display, handset or other hardware problems on page 309
- Digital telephone display is unreadable on page 309
- Telephone has no dial tone on page 310

Telephone has faulty buttons, display, handset or other hardware problems

Run a Station Set Test (Feature 8 0 5).

Digital telephone display is unreadable

If the trouble is with an M7310 or an M7324 telephone

1. Press Feature * 7.
2. Press **UP** or **DOWN** to adjust the display contrast to the desired level.
3. Press **OK**.

If the trouble is with an M7100 telephone

1. Press Feature * 7.
2. Press a number on the dial pad to adjust the display contrast to the desired level.
3. Press Hold.

If the display is still unreadable, disable the telephone and replace it with a known working one and enable the working telephone. Disable the telephone using the following procedure:

1. Choose **Resources, Media Bay Modules** and then the appropriate bus.
2. From **Ports on Bus**, select the port on the bus that the telephone uses.
3. Select **Channels**.
4. Select the channel that the telephone uses.
5. From the Configuration menu, select **Disable**.

To enable the working telephone, use the preceeding procedure and select **Enable** from the Configuration menu.

Telephone has no dial tone

1. Run a Station Set Test **(**Feature 8 0 5**)**.
2. Check for dial tone.
3. Check the display.
4. If the problem persists, replace the telephone with a known working telephone of the same type (so that the programming is retained).
5. Check the internal wiring at both the modular jack and the distribution cross-connect. A TCM port should have between 15 and 26 V DC across the Tip and Ring when the telephone is disconnected.
6. Check the line cord.

Problems with lines

The troubleshooting problems listed here focus on trouble with making calls or using lines. For more information, refer to one of the following problems:

- Calls can be received but cannot be made on page 310
- Dial tone is absent on external lines on page 311
- Lines at a telephone are busy after call is over on page 311
- Auto-answer line rings at a telephone on page 313
- Prime telephone gets misdialed calls on page 314
- Selected lines reads “Not in service” or “Not available” on page 314
- Selected line pool shows “No free lines” on page 315

Calls can be received but cannot be made

1. If an incorrect line number or name appears (or if neither appears) on the telephone display, check the programming settings.
   OR
   If the correct line number or name appears on the telephone display, make sure the external lines are properly cross-connected.
2. Check external lines by attaching a test telephone directly on the distribution block.

3. Ensure that the 25-pair cable is properly connected from the EE-DSM to the station set termination.

4. In the Unified Manager, verify that the EE-DSM module is not disabled or unequipped by selecting **Resources, Media Bay Modules** and the bus that the module is on. For more information, refer to Display the Media Bay Module status on page 279.

5. Disable and then enable the module by selecting **Resources, Media Bay Modules** and the bus that the module is on. For more information, refer to Disable a module on page 279 and Enable a module on page 280.

6. If you still cannot make external calls, power down, then power up the system. This should be done after business hours to avoid losing calls.

7. To check the line, contact the telephone company.

Notify service provider of T1 signaling disruption.
Notify your T1 service provider before disconnecting your T1 lines, removing power to your system, or performing any other action that disrupts your T1 signaling. Failure to notify your T1 service provider may result in a loss of T1 service.

Dial tone is absent on external lines

1. Check for dial tone using a test telephone at the connections for the external line on the distribution block.

2. Make sure that a trunk module for the line is properly installed in the server or expansion cabinet.

3. Make sure that the hub is properly connected to the MSC card.

4. In the Unified Manager, select **Resources, Media Bay Modules** and the bus that the module is on, to ensure that the line is not disabled. See Display the Media Bay Module status on page 279.

Lines at a telephone are busy after call is over

Line indicators that have been solid for a long time are the only visible indication that lines are hung. The problem may be due to one of the following:

- A redirected line remains busy on page 312
- Programming is incorrect on page 312
- Lines require maintenance session on page 312

A redirected line remains busy

A line that has been redirected using Line Redirection may, under some circumstances, remain busy after a call is over. If this happens, the outgoing line for the redirection also remains busy. You can clear this kind of hung line only at the telephone that was used to redirect the line.

Use the following procedure to clear the line:

1. Enter the Button Inquiry feature code (Feature * 0) at the telephone that was used to redirect the line.

2. Press the button of the redirected line.

3. Press SHOW or #.

4. Press DROP or *.

Both the redirected line and the outgoing line for the redirection should now be cleared.

Programming is incorrect

The supervision and/or disconnect timer programming for the line do not match the settings for the line at the central office.

Verify in the Unified manager that your programming for the line matches the central office settings using the following procedure:

1. Choose **Services**, **Telephony Services**, **Lines**.

2. Select the affected line.

3. Select **Trunk/Line data**.

   The line's programming data is displayed.

4. Verify that the supervision and disconnect timer programming match the settings for the line at the central office.

Lines require maintenance session

Lines are still hung after all the above solutions have been investigated or tried out.

For lines that are hung for any other reason, you will have to run a Maintenance session and disable then re-enable the affected trunk module using the following procedure:

1. Choose **Resources, Media Bay Modules** and the bus that the module is on. Disable the module using the procedure, Disable a module on page 279.

2. Enable the module using the procedure, Enable a module on page 280.

Follow the procedures in the Basic troubleshooting procedure on page 306 before proceeding.

Auto-answer line rings at a telephone

The problem may be due to one of the following:

- Installed hardware does not support disconnect supervision on page 313
- Line is configured as auto-answer and unsupervised on page 313
- Line is not equipped for disconnect supervision at the central office on page 313
- Trunk module's disconnect timer setting is not correct on page 314

Installed hardware does not support disconnect supervision

You configured a loop start trunk as auto-answer but the installed hardware does not support disconnect supervision. (In this case, the symptom would be accompanied by the Alarm 62 code symptom.) If the installed hardware does not support disconnect supervision, reconfigure the trunk as manual-answer.

Line is configured as auto-answer and unsupervised

If the line is configured as auto-answer, reconfigure it as manual-answer. If the line is configured as unsupervised, reconfigure it as supervised. Use the following procedure.

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Select the affected line.
3. Select **Trunk/line** data.
4. In the **Trunk mode** field, reconfigure the line as supervised by selecting **Super** from the drop-down menu.

   OR

   In the **Auto answer** field, reconfigure the line as manual answer by selecting **Manual** form the drop-down menu.

Line is not equipped for disconnect supervision at the central office

If the line is not equipped for disconnect supervision at the central office, reconfigure the trunk as manual-answer using the following procedure:

1. Choose **Services**, **Telephony Services**, **Lines**.
2. Select the affected line.

3. Select **Trunk/line** data.

4. In the **Auto answer** field, reconfigure the line as manual answer by selecting **Manual** form the drop-down menu.

Trunk module's disconnect timer setting is not correct

If the disconnect timer setting for the trunk module does not match the setting for the line at the central office, reconfigure it to match the setting using the following procedure:

1. Choose **Services**, **Telephony Services**, **Lines**.

2. Select the affected line.

3. Select **Trunk/Line data**.

   The data is displayed for this line.

4. In the **Trunk mode** field, select the correct setting from the drop-down menu.

For more information, refer to Trunk/line data on page 111, Trunk mode.

Prime telephone gets misdialed calls

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. The call has been routed to the prime telephone for the incoming trunk. Perform the following steps to determine the cause:

1. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.

2. Verify all the digit strings that the switch should be sending.

3. Check that you have defined the corresponding Received number for every target line in your system.

4. Make sure that the published telephone numbers for your network are correct.

Selected lines reads "Not in service" or "Not available"

The problem may be due to one of the following:

- Line is connected to an EE-DTM which is currently not in service on page 315
- Line has been disabled for maintenance purposes on page 315
- Line has not been provisioned on page 315

Line is connected to an EE-DTM which is currently not in service

Perform the following steps to determine why the EE-DTM is not in service:

1. Check if the green LED on the EE-DTM is flashing to indicate that service is suspended.

2. Check if any yellow LEDs are on to indicate an alarm or error condition.

3. Check if the red test LED is on to indicate that a continuity loopback test is running.

4. Check that the cable connecting the EE-DTM to the termination point from the central office or network is properly connected.

5. Check that the EE-DTM is properly inserted in the module bay.

6. In the Unified Manager verify the status of the EE-DTM. For more information, refer to the procedure, Display the Media Bay Module status on page 279.

Line has been disabled for maintenance purposes

If the line has been disabled, enable the line. If the line will be out of service for some time, configure another line to replace it on the telephone.

Line has not been provisioned

If the line has not been provisioned, provision it.

Selected line pool shows "No free lines"

If this happens often, there are not enough lines in the line pool to serve the number of line pool users. If this is the case, and the line pool contains loop start trunks, move the under-utilized loop start trunks from other line pools into the deficient line pool.

Problems with optional equipment

For more information on problems with optional equipment attached to the Enterprise Edge system, refer to one of the following problems

- Problems with the Enterprise Edge ATA 2 on page 316
- Problems with the auxiliary ringer on page 316
- Problems with external paging on page 317
- Problems with Music on Hold and Background Music on page 317

Problems with the Enterprise Edge ATA 2

1. Check the connections to the jack.

2. Check the connections to the Enterprise Edge ATA 2.

3. Disconnect the Enterprise Edge ATA 2 and replace it with a working digital telephone. If the telephone still works properly, the system and the EE-DSM are operating properly.

4. Verify that the programming has been performed correctly.

5. If the trouble seems to be in the system or EE-DSM, double-check all wiring and programming options.
   OR
   If the trouble seems to be with the Enterprise Edge ATA 2, disable the Enterprise Edge ATA 2 and replace it with a known working one.

For more information, refer to the *Enterprise Edge ATA 2 Installation Guide*.

Running a Maintenance session to test a Enterprise Edge ATA 2

1. Choose **Resources, Media Bay Modules** and navigate through the selections to find the ATA 2, to ensure that the Enterprise Edge ATA 2 is not disabled. See Identify a device connected to the system on page 280.

2. Disable the port connected to the Enterprise Edge ATA 2 using the procedure, Disable a device on page 281.

3. Enable the port connected to the Enterprise Edge ATA 2 using the procedure, Enable a device on page 281.

Problems with the auxiliary ringer

1. If the auxiliary ringer is used for Schedules (Night, Evening, or Lunch service), ensure that Schedules is activated from the control telephone.

2. Check the wiring between the auxiliary ringer generator and the ringing device. Refer to the auxiliary ringer wiring chart.

3. Check the following wiring between the auxiliary ringer generator and the distribution block.

4. Ensure that the auxiliary ringer contacts are operating properly by checking with an ohmmeter across the auxiliary ringer pin contacts listed above.

5. Check that the auxiliary ringer pin contacts are programmed to operate in conjunction with any or all of the features in the auxiliary ringer programming chart.

   The current capacity of the Enterprise Edge relay contacts is 5 0mA DC. They are designed to operate with the auxiliary ringer generator, or equivalent.

Problems with external paging

1. Use the Button Inquiry feature **(**Feature * 0**)** to verify the feature of a programmable memory button.

2. Check the wiring between the 50-pin connector and the paging amplifier.

3. Test external paging Feature 6 2 to ensure that it is working. The nominal output signal from the Enterprise Edge is 100 mV ac r o s s 6Ω0

Problems with Music on Hold and Background Music

Although Music on Hold and Background Music are separate features, they share the same wiring and customer-supplied music source.

1. Ensure that the proper feature access code **(**Feature 8 6**)** is turned on. Adjust the volume using the volume control bar.

2. Use the Button Inquiry feature **(**Feature * 0**)** to verify the feature on a programmable memory button.

3. If there is trouble with Music on Hold or Background Music, check the feature settings in the Unified Manager by selecting **Services, Telephony Services**, **General settings** and then **Feature settings**.

4. Check the wiring between the music source and the 50-pin connector.

5. Ensure that the music source is turned on, is operational, and the volume control is set properly.

6. Any music source with a low-output impedance (for example, less than 3,300 ohms) can be connected. The output level must be less than one volt.

Problems with module service

Check first for user problems, then wiring connections and programming errors before replacing Enterprise Edge equipment.

Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

1. Check that the module is properly inserted in the server or expansion cabinet.

2. Access **Services, Telephony Services** and then **Feature settings**, to ensure that the module is not disabled. For more information, refer to the procedure, Display the Media Bay Module status on page 279.

If the problem persists
If the AC power is present and the LED indicator on the module is off, contact your customer service representative. If AC power is present and the LED indicator on the Enterprise Edge system is off, replace the system power supply.

Note: Before you replace the system power supply, disconnect all central office and station lines from the Enterprise Edge system. Power down the system by unplugging it.

Refer to *Enterprise Edge Installation and Maintenance Guide* for information on replacing components.

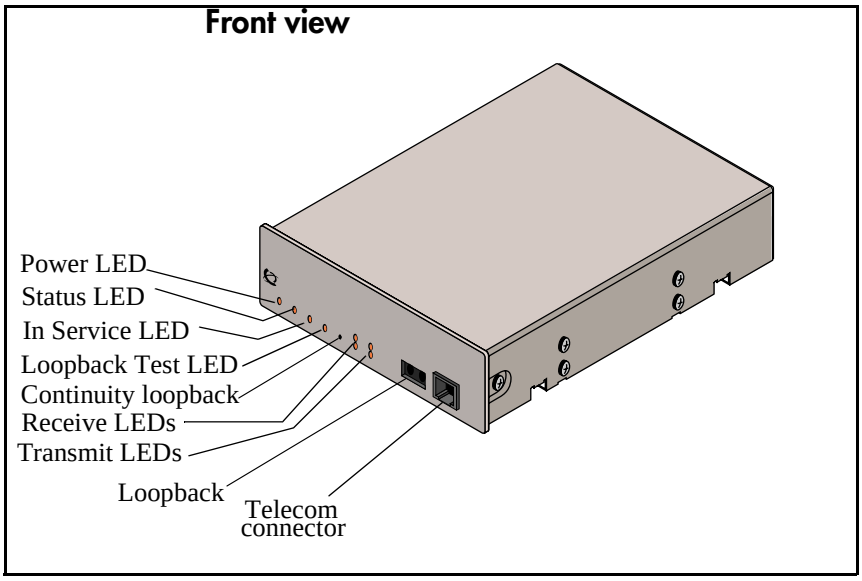
Refer to the following sections for more information:

- Digital Trunk Computer Module trouble on page 318
- Monitoring the T1 or PRI signal on page 320

Digital Trunk Computer Module trouble

1. Choose **Resources, Media Bay Modules** and the bus that the module is on to verify that the EE-DTM is enabled and that it's lines are provisioned. For more information, refer to the procedure, Display the Media Bay Module status on page 279.

2. Check the LEDs on the front of the EE-DTM



- **Receive Alarm**: yellow LED on indicates a problem with the digital transmission being received. This half-duplex link is unusable.
- **Receive Error**: yellow LED indicates a minor error as a result of degraded digital transmission. Possible causes are an ohmic connection, water ingress, or too long a loop.
- **Transmit Alarm**: red LED on indicates an inability to transmit. Alarm indication signal (AIS) is being transmitted to the terminating switch. This half-duplex link in unusable.
- **Transmit Error**: yellow LED on indicates a remote alarm indication (RAI) carrier failure alarm (CFA) is being sent to the terminating switch. If the Transmit Alarm is not on, this indicates a far-end or cable problem.
- **In service**: flashing green indicates that the T1 or PRI trunks are out of service because of a running loopback test, or because the EE-DTM is being initialized.
- **Loopback test**: red LED on while a continuity loopback test is running.
- **All LEDs flashing continuously**: the EE-DTM is being initialized.

3. In the Unified Manager, select **Resources, Telephony**, **Maintenance**, and **Tests** to run any loopback tests as appropriate.

4. Check the pinout of the cable that connects the EE-DTM to the termination point from the T1 or PRI service provider or the external channel service unit, and check that the cable is properly connected.

5. Check with your T1 or PRI service provider to see if through-fed repeaters are used on the T1 or PRI span. The EE-DTM does not provide the DC connection required for through-fed repeaters. If through-fed repeaters are used on the T1 span, disable the internal CSU and connect the EE-DTM to an external CSU.

6. If the problem persists, replace the EE-DTM.

Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

For information on how to replace any system components, refer to the *Enterprise Edge Installation and Maintenance Guide*

Monitoring the T1 or PRI signal

If you are finding minimal faults with the T1 or PRI signal, you can monitor the signal to try and isolate the problem. The monitor jack on the EE-DTM faceplate provides non-intrusive, bridged in-service monitoring of the T1 or PRI signal. Connect a protocol analyzer or other test equipment into the monitor jack to monitor the signal received from the network, and the signal transmitted by Enterprise Edge.

Problems with Trunk or Station Modules

1. Choose **Resources, Media Bay Modules** and the bus that the module is on to ensure that the module is not disabled. For more information, refer to the procedure, Display the Media Bay Module status on page 279.

2. Disable the module using the procedure, Disable a module on page 279.

3. Enable the module using the procedure, Enable a module on page 280.

4. For an EE-DTM, EE-CTM or EE-DSM:

   Check the external line by terminating a single-line telephone directly on the distribution block, or equivalent, which connects to the Trunk Module.

5. For the EE-ASM:

   If the EE-ASM is still down, power down, then power up the Enterprise Edge system.

If the problem persists

1. If AC power is present and the LED indicator on the module is off, replace the module.
2. Replace the link cable.
3. Replace the module.
4. Replace the MSC.

For information on replacing components, refer to the *Enterprise Edge Installation and Maintenance Guide*.

Problems for network or remote users

Refer to one of the following items for information on how to solve network or remote user problems.

- Remote feature code gets no response on page 321
- Dialed number gets ringback and the wrong person on page 322
- Dialed number gets dial tone instead of ringback on page 322
- Dialed number gets busy tone on page 322
- Dialed number does not get through on page 322
- Dialed feature code gets overflow tone on page 323
- Dialed feature code gets busy tone on page 324
- Line pool access code gets overflow tone on page 324
- Line pool access code gets ringback on page 325
- Line pool access code gets busy tone on page 325
- Dialed number gets no response on page 325

Remote feature code gets no response

An Enterprise Edge user has called into another Enterprise Edge system and is trying to activate a remote feature but gets no response after dialing the feature code. Perform the following steps to determine the cause:

1. Make sure that the remote caller is dialing the feature code correctly. Use the asterisk (*) character, followed by the feature code, to activate a remote feature. (Do not use **Feature** for accessing features on a remote Enterprise Edge system.)
2. Make sure that the remote user is dialing tones, not pulses once the call is answered.

Dialed number gets ringback and the wrong person

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. The call has been routed to the prime telephone for the incoming trunk. Perform the following steps to determine why calls are being routing incorrectly:

1. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.

2. Verify all the digit strings that the switch should be sending.

3. Check that you have defined the corresponding Received number for every target line in your system.

4. Make sure that the published telephone numbers for your network are correct.

Dialed number gets dial tone instead of ringback

The remote caller has tried to reach an Enterprise Edge target line, but has reached the Enterprise Edge system instead. The system has mapped the incoming digits onto the Auto DN. Perform the following steps to determine why the remote caller cannot reach the target line:

1. Verify all the digit strings that the switch should be sending.

2. Check that you have defined the corresponding Received number for every target line in your system.

3. Check that you have defined the correct Auto DN for your system.

4. Make sure that the published telephone numbers for your network are correct.

Dialed number gets busy tone

The target line that the incoming digits map onto is busy, and there is no prime telephone for the incoming trunk. For maximum call coverage, make sure that you configure a prime telephone for every incoming trunk.

Dialed number does not get through

The problem may be due to one of the following:

- Digits do not match Received number or Auto DN on page 323
- The Enterprise Edge system did not receive some or all of the incoming digits on page 323

Digits do not match Received number or Auto DN

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. There is also no prime telephone assigned for the incoming trunk. In this case, the caller may hear overflow tone from the Enterprise Edge system or a recorded message from the originating switch. Perform the following troubleshooting steps:

1. Configure a prime telephone for every incoming trunk.
2. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
3. Verify all the digit strings that the switch should be sending.
4. Check that you have defined a Received number for every target line in your system.
5. Make sure that the published telephone numbers for your network are correct.

The Enterprise Edge system did not receive some or all of the incoming digits

Perform the following troubleshooting steps to determine why the system is not receiving some of the incoming digits:

1. Check that the system hardware is receiving signals properly.
2. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
3. If the switch at the far end is sending pulse signals, make sure they are being sent at the proper rate. (Pulse digits must be 3 0 0ms or more apart for the Enterprise Edge system to receive them.)

Dialed feature code gets overflow tone

The problem may be due to one of the following:

- Remote caller does not have access to that feature on page 323
- Feature code is not valid on page 324
- Call may originate on a telephone that uses pulse signaling on page 324

Remote caller does not have access to that feature

Check the remote package that you assigned to the incoming trunk. Make sure that it gives the appropriate access to the remote caller.

Feature code is not valid

1. Make sure that remote callers have a correct listing of the features that are programmed for remote access.

2. Ensure that remote callers are programming the feature code correctly. Press * followed by the feature code to activate a remote feature.

Call may originate on a telephone that uses pulse signaling

The caller may be dialing on a rotary-dial telephone or on a push-button telephone that uses pulse signaling. Inform remote callers that they must dial from a push-button telephone that uses DTMF “tone” signaling.

Dialed feature code gets busy tone

A resource that the remote feature uses may currently be in use. For example, a remote caller trying to use the paging feature would get a busy tone if the auxiliary speaker were being used at the time.

If repeated attempts to use the remote feature get busy tone, there may be a malfunction in a resource that the feature uses. Check that the remote feature hardware is functioning normally.

Line pool access code gets overflow tone

The problem may be due to one of the following:

- Remote caller does not have access to line pool on page 324
- Line pool access codes are invalid on page 324
- Call may originate on a telephone that uses pulse signaling on page 325

Remote caller does not have access to line pool

If the published line pool access code is valid, the remote caller does not have access to that line pool. If this is the case, change the remote package for the incoming trunk so that it permits access to that line pool. Alternatively, give the remote caller a line pool access code that is permitted within the Class of Service on the incoming trunk.

Line pool access codes are invalid

If the published line pool access code is invalid, the system has attempted, without success, to match the invalid code to an Enterprise Edge target line internal number, and there is no prime telephone for the auto-answer trunk. Verify the following:

1. Published line pool access codes are correct.

2. Check that the line pool access codes have been entered correctly under **Access codes** in **System programming**.

Call may originate on a telephone that uses pulse signaling

The caller may be dialing from the network on a rotary-dial telephone or on a push-button telephone that uses pulse signaling. Inform remote callers that they must dial from a push-button telephone that uses DTMF “tone” signaling.

Line pool access code gets ringback

If the line pool access code gets ringback, the published line pool access code is invalid, and the system has routed the call to the prime telephone for the incoming trunk. Verify the following:

1. Make sure that the published line pool access codes are correct.

2. Check that the line pool codes have been entered correctly under **Services**, **Telephony Services**, **General Settings**, **Access codes**.

Line pool access code gets busy tone

The line pool access code will get a busy tone if there are not enough lines in the line pool to serve the number of users. If the line pool contains loop start trunks, enter programming and move under used loop start trunks from other line pools into the deficient line pool. Alternatively, you can create a separate line pool for remote users only.

Dialed number gets no response

This may be caused by one of the following:

- Remote caller dials before far end is ready on page 325
- Line malfunction on page 325
- System malfunction on page 325

Remote caller dials before far end is ready

The remote caller, after accessing a line in a line pool, may have started dialing before the far end was ready to receive digits. To avoid this problem, instruct remote callers to wait until they hear feedback before entering any digits.

Line malfunction

There may be a malfunction in the line that the remote caller accessed. If the problem is persistent, check that all lines in the affected line pool are functioning normally.

System malfunction

There may be a malfunction in the system that the caller is trying to reach. Inform the operators of the system at the far end that the dialed number is not getting through.

Problems with Companion sets (North American systems only)

When there is a problem with a Companion set:

1. Make sure the portable is compatible with Enterprise Edge Voice Messaging Companion Wireless software.

2. Verify that the portable is ON and that the battery is not low.

3. Establish a radio connection to get a dial tone.

4. If there is no dial tone present:

   - verify that a dial tone is available from Enterprise Edge.
   - the portable may not be registered. If this is the case, register the portable again.
   - check that the portable is using the correct registration slot.
   - verify that the portable has been assigned the correct internal number by calling it from another telephone.

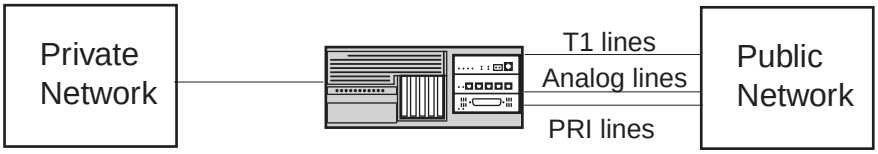
Appendix A: Network Examples

In addition to public network connections, Enterprise Edge can be integrated into an existing private network of M1s to form a corporate telecommunications network.

Tips

The ability to perform private networking requires software keys for Enterprise Edge VoIP Gateway and Enterprise Edge PRI.

Enterprise Edge uses enhanced trunking to join other Nortel or customer equipment in a private network. Authorized users can also access tie lines, central office lines, and Enterprise Edge features from outside the system.



Enterprise Edge

For background information on Enterprise Edge networking, refer to the following:

- Access using Enterprise Edge on page 328
- Lines used for networking on page 328
- Remote system access to Enterprise Edge on page 330
- Enterprise Edge security on page 333

For more information on setting up dialing plans and examples of Enterprise Edge networking, refer to

- Coordinated dialing plans on page 335
- Networking examples on page 341
- Public networking scenarios on page 362
- Private networking scenarios on page 365

Access using Enterprise Edge

Callers using Enterprise Edge can:

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network
- select an outgoing central office line to access the public network
- use all of the Enterprise Edge features.

Callers in the public network can:

- call directly to one or more Enterprise Edge telephones
- call into Enterprise Edge and select an outgoing tie line to access a private network
- call into Enterprise Edge and select an outgoing central office line to access the public network
- call into Enterprise Edge and use remote features.

Callers in the private network can:

- call directly to one or more Enterprise Edge telephones
- call into Enterprise Edge and select an outgoing tie line to access other nodes in a private network
- call into Enterprise Edge and select an outgoing central office line to access the public network
- call into Enterprise Edge and use remote features.

Lines used for networking

External lines provide the physical connection between Enterprise Edge and other systems in a private or public network. Lines are numbered 061 to 238. Lines 001 to 008 are used for Enterprise Edge VoIP Gateway (IP telephony functionality). Enterprise Edge includes different types of modules that are configured for different types of lines:

- A DTI (EE-DTM) configured for PRI and BRI is used for incoming and outgoing calls (two-way DID). Incoming calls are routed directly to an Enterprise Edge telephone. Outgoing calls are made using the intercom key and dialing destination codes.
- A DTI (EE-DTM) configured for T1 has digital lines that are configured as Groundstart, E&M, Loop, and DID.

Target lines are virtual communication paths between trunks and telephones on the Enterprise Edge system. They are incoming lines only, and cannot be selected for outgoing calls. With target lines, you can concentrate incoming calls on fewer trunks. This type of concentration is an advantage of DID lines. Enterprise Edge target lines allow you to direct each DID number to one or more telephones. Target lines are numbered 241 to 336.

Telephones can be configured to have an appearance of any type of trunk and line (including target lines, excluding PRI trunks). If assigned, they are used for monitoring call usage.

For more information on Enterprise Edge external line types, refer to:

- PRI lines on page 329
- T1 lines (Loop, E&M, DID, Ground start) on page 329
- BRI lines on page 330
- DPNSS lines (International systems only) on page 330

PRI lines

Primary Rate Interface (PRI) lines give you incoming and outgoing access to an ISDN network and are auto-answer trunks. PRI lines are set to auto-answer by default and cannot be changed. The DTI (EE-DTM) is configured to provide PRI lines.

PRI lines provide a fast, accurate and reliable means of sending and receiving data, images, text and voice information. Using PRI lines allows for faster transmission speeds and the addition of a variety of powerful business applications, including remote LAN access, video conferencing, file transfer and Internet access.

T1 lines (Loop, E&M, DID, Ground start)

Ground start lines offer the same features as loop start trunks, but are used when the local service provider does not support disconnect supervision for the digital loop start trunks. Ground start trunks work with T1 only. By configuring lines as ground start, the system will be able to recognize when a call is released at the far end.

Tips

You cannot change the trunk mode for a ground start trunk on an EE-DTM (or DTI). It always has disconnect supervision.

An EE-DTM configured for T1 can provide a maximum of 24 ground start trunks. Analog ground start trunks are not supported.

Target lines are assigned by default for all templates except the DID template.Target lines are assigned line numbers (for example, 241 to 336) similar to physical lines.

You can program auto-answer T1 loop start, T1 E&M trunks, T1 DID, T1 ground start trunks, PRI, and IP trunks to map to target lines to provide for attendant bypass (calling directly to a department or individual) and line concentration (one trunk can map onto several target lines).

BRI lines

Basic rate interface (BRI) lines give you incoming and outgoing access to an ISDN network. ETSI ISDN BRI is the European Telecommunications Standards Institute specification for BRI ISDN service. BRI provides 2 bearer B-channels operating at 64 kbits/s and a data D-channel which operates at 16 kbits/s. The D-channel is used primarily to carry call information. Like loop start trunks, BRI lines can be configured as manual-answer or auto-answer.

DPNSS lines (International systems only)

Digital Private Network Signalling System (DPNSS) lines, when installed in a network, offer significant enhancements to Enterprise Edge networking capabilities.

DPNSS makes it easier to support centralized network functionality within private networks, for operators and attendants dealing with large numbers of calls. Its routing capabilities provide more of the larger-network capabilities without the expense of installing a new system, re-configuring all the nodes and worrying about a lot of downtime. Most functionality over DPNSS lines is transparent once the DPNSS is programmed into the system.

DPNSS allows a local node, acting as a terminating node, to communicate with other PBXs over the network using E1 lines. For example, corporate offices separated geographically can be linked over DPNSS lines to other Enterprise Edge systems, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Enterprise Edge systems to function like a private network.

Remote system access to Enterprise Edge

The remote access feature allows callers elsewhere on the private or the public network to access Enterprise Edge by dialing directly without going through an attendant. Once in the system, the remote user can use some of the system's resources. The remote access must be enabled in programming before callers can use it.

Enterprise Edge supports remote system access on a number of trunk types which may require the remote caller to enter a password for direct inward system access (DISA).

The system resources (dialing capabilities, line pool access and feature access) that a remote user may access depends on the Class of Service (COS) assigned to them. See COS Passwords on page 160 and the *Nortel Networks Voice Programming Guide* for more details.

Note: To use features on Enterprise Edge remotely, press * followed by the Feature code. Even if you are calling from another Enterprise Edge system, press * instead of Feature.

For more information on remote system access on various trunk types, refer to:

- Remote access on loop start trunks on page 331
- Remote access on a private network on page 331
- Remote access on T1 Direct Inward Dial (DID) trunks on page 332
- Remote access on PRI trunks on page 332
- Remote access on DPNSS lines on page 332

Remote access on loop start trunks

Loop start trunks provide remote access to Enterprise Edge from the public network. They must be configured to be auto-answer to provide remote system access.

A loop start trunk **must** have disconnect supervision if it is to operatein auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer, the system answers with system dial tone and no (COS) password is required. In this case, control over the system capabilities available to the caller is provided only by the restriction filters assigned to the line.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a COS password which determines which system capabilities are available to the caller.

Remote access on a private network

Nodes on the private network deliver the last dialed digits to the destination Enterprise Edge node for interpretation. The destination Enterprise Edge node either matches the digits to a target line or interprets the digits as a remote feature request. The call is either routed to the specified target line, or the remote feature is activated.

By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are **not** answered with DISA.

If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a COS password.

The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in Access codes on page 156 of the Configuring Enterprise Edge Services chapter.

Remote access on T1 Direct Inward Dial (DID) trunks

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- a remote caller is on the public network dialing standard local or long-distance telephone numbers
- the digits received are delivered by the central office
- DISA cannot be administered to a T1 DID trunk

As with a private network, the dialed digits may be programmed to match those of a specific target line DN, the DISA DN or the Auto DN.

Remote access on PRI trunks

Remote system access on PRI trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- a remote caller is on the public network dialing standard local or long-distance telephone numbers
- the digits received are delivered by the central office
- answer with DISA cannot be administered to a PRI trunk

As with a private network, the dialed digits may be programmed to match those of a specific target line DN, the DISA DN or the Auto DN.

Remote access on DPNSS lines

A remote caller can access a Enterprise Edge system dial tone, select a line pool that contains exchange lines or DPNSS lines, then dial a number. The procedure is identical to dialling an outside number from an extension in the local system. The main features are:

- Calls coming from another switch to the Enterprise Edge system can be routed in two ways, depending on the Answer mode that you program. If Answer mode is set to Manual and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If Answer mode is set to Auto, the incoming call is answered automatically by the CCU. Because most other DPNSS features are extension specific, it is recommended that all DPNSS lines be configured as Auto-answer lines.
- The Page feature is available to both remote callers and callers within the system. The operation of the feature is identical, however the remote caller must have DTMF capability to access the feature.
- Line Redirection allows the originating party to redirect a call, waiting a connection or re-connection, to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Enterprise Edge security

Programming provides several ways of protecting Enterprise Edge from unauthorized access or use. For more information on features that provide restricted access to your Enterprise Edge system, refer to:

- Class of Service on page 333
- Restriction filters on page 333
- Direct inward system access (DISA) on page 335

Class of Service

Class of Service (COS) refers to the capabilities that Enterprise Edge provides to users who access the system from the public or a private network. The COS includes:

- filters that restrict dialing on the line
- an access package, which defines the set of line pools that may be accessed and whether or not the user has access to the paging feature.

The COS that is applied to an incoming remote access call is determined by:

- the filters that you apply to the incoming trunk
- the COS password that the caller used to gain access to Enterprise Edge.

In cases where DISA is not automatically applied to incoming calls, the remote caller can change the COS by dialing the DISA DN and entering a COS password. To program COS passwords, see COS Passwords on page 160.

Restriction filters

Restriction filters can be used to restrict the numbers that may be dialed on any external line within Enterprise Edge. Up to 100 restriction filters can be created for the system. A restriction filter consists of up to 48 restrictions and their associated overrides.

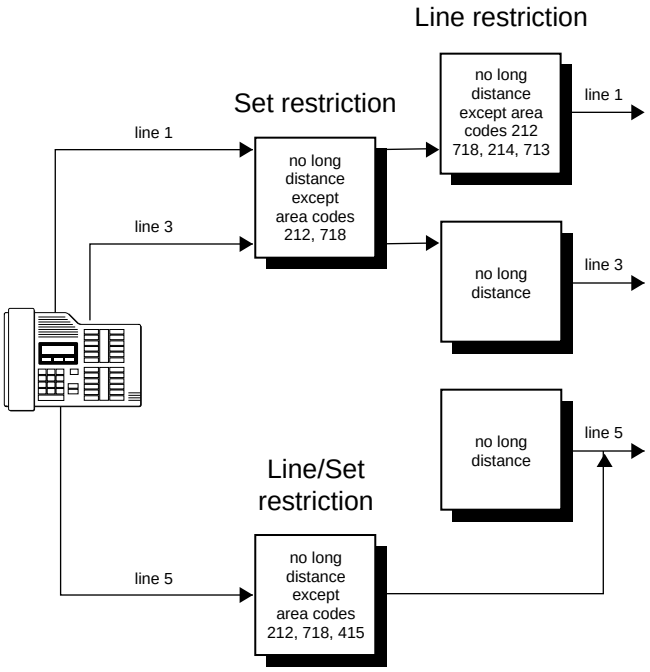
To restrict dialing within the system, you can apply restriction filters to:

- outgoing external lines (as line restrictions)
- telephones (as set restrictions)
- external lines on specific telephones (as line/set restrictions)

Restriction filters can also be specified in Restrictions service for times when the system is operating according to a schedule. See Restriction service on page 141 and Restriction filters on page 124 for more details. Dialed digits must pass both the line restrictions and the set restrictions. The line per set (line/set) restriction overrides the line restriction and set restriction.

Line and set restrictions are shown in Line restriction example on page 334 and Remote line restriction example on page 334.

Line restriction example

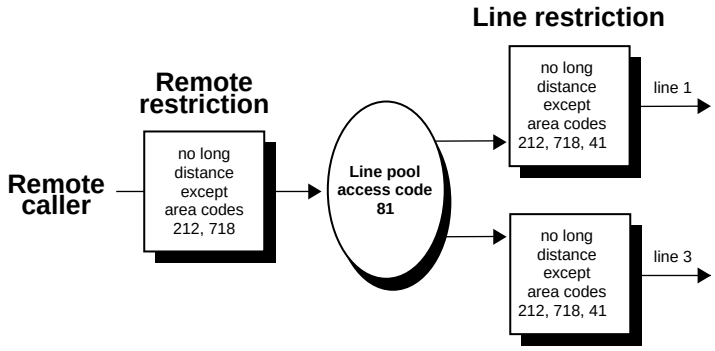


In this diagram, a caller using line 001 could only dial long-distance numbers to area codes 212 and 718. A caller using line 003 could not dial any long-distance numbers. A caller using line 005 could dial long-distance numbers to area codes 212, 718, and 415.

Tip

To restrict dialing from outside the system (once a caller gains remote access), apply restriction filters to incoming external lines (as remote restrictions).

Remote line restriction example


Line restriction
Remote restriction
Remote caller
no long distance except area codes 212, 718
Line pool access code 81
no long distance except area codes 212, 718, 41
line 1
no long distance except area codes 212, 718, 41
line 3

In this case, dialed digits must pass both the remote restriction and the line restriction. A remote caller can override these filters by dialing the DISA DN and entering a COS password.

Direct inward system access (DISA)

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a COS password that determines what they are allowed to do in the system.

Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default. For DISA programming instructions.

Tips

T1 DID trunks cannot be configured to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.

Coordinated dialing plans

Enterprise Edge has a routing feature that allows you to set up a coordinated dialing plan with other systems in the public network. The goal is to have a network-wide dialing plan where all telephone numbers are unique and of a uniform length.

Coordinated dialing plans are typically used with a network of systems with a three to seven digit dialing access between them.

Any programming for routing should be carefully planned using tables. For more information about routing and destination codes, see Routing Service on page 142. This section deals with applying the programming in network situations.

For more information on Enterprise Edge dialing plans, refer to:

- Dialing plan using public lines on page 335
- Dialing plan using T1 E&M lines on page 337
- Dialing plans with shared line pools on page 340

Dialing plan using public lines

The following illustrations provide an example of how you might record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax and Vancouver. Without routing, an Enterprise Edge user in Toronto would have to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number (referred to as “External #” in programming), the user simply dials 3027. The same feature is available for Vancouver (604).

In the column Dial out, P stands for pause, a host system signaling option. Press Feature 7 8 to insert a 1.5 second pause in the dialing string.

Routing Service (Services: Routing Service)

Route # (000-999)	Dial out (if required) (max. 24 digits or characters)	Use Pool
100	1-P-902-585	A B C
101	1-P-902-585	A B C
102	1-P-604-645	A B C
103	1-P-604-645	A B C
		A B C

Routing service (continued)

Dest code (Services: Routing service: Dest codes)

Service Schedule	Normal		Sched 1		Sched 2		Sched 3	
Sched name (max. 7 char.)	Normal		Night		Evening		Lunch	
DestCode (max. 7 digits)	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length
30	~~000~~100	~~All~~ 0	000	All	000	All	000	All
31	~~000~~101	~~All~~ 0	000	All	000	All	000	All
32	~~000~~102	~~All~~ 0	000	All	000	All	000	All
33	~~000~~ 103	~~All~~ 0	000	All	000	All	000	All

Destination code numbering in a network

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits. The following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
8	Call Park Prefix
9	All PSTN Calls

In the table, 4 is used as the initial digit for the coordinated dialing plan, but 5, or 6 could also be used for this purpose.

Tip

When programming a button to dial a Network number automatically (autodial), network calls must be programmed as external autodial numbers, even though they resemble internal extension numbers.

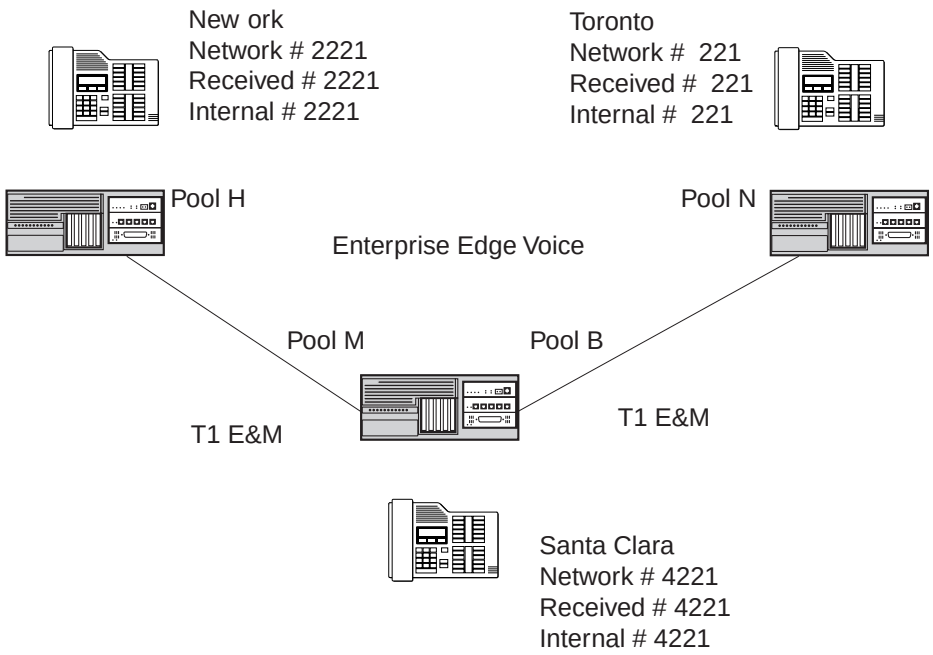
Routes generally define the path between the Enterprise Edge system and another switch in the network, not other individual telephones on that switch.

Dialing plan using T1 E&M lines

By properly planning and programming routing tables and destination codes, an installer can create a dialing plan where T1 E&M lines between Enterprise Edge systems are available to other systems in the network

Dialing plan for Enterprise Edge network on page 337 shows a coordinated dialing plan for a network of three Enterprise Edge systems. Each system must be running Enterprise Edge software. Each system must be equipped with target lines and Enterprise Edge with an EE-DTM with at least one T1 E&M line. Programming information for this network is shown in Routing information on page 338.

Dialing plan for Enterprise Edge network



Routing information

Heading	Parameter	Setting
New York office:		
Trunk/Line Data	Line 061	T1 E&M
	Answer Mode	Auto
	Line type	Pool H
	Line 241	Target line
	Received #	2221
Line Access	Set 2221	L241: Ring only
	Line pool access	Line pool H
To Santa Clara:		
Routing service	Route	001
	Use	Pool H
	External #	None
	Destination Code	4
	Normal route	001
	Absorb	None
To Toronto:		
Routing service	Destination Code	6
	Absorb	None
	Normal route	001
Santa Clara office:		
Trunk/Line Data	Line 091	T1 E&M
	Answer Mode	Auto
	Line type	Pool M
Trunk/Line Data	Line 092	T1 E&M
	Answer Mode	Auto
	Line type	Pool B
	Line 251	Target line
	Received #	4221
Line Access	Set 4221	L251: Ring only
	Line pool access	Line pool B Line pool M
***To New York*:**		
Routing service	Route	001
	Use	Pool M
	External #	None
	Destination Code	2
	Absorb	None
	Normal route	001

Heading	Parameter	Setting
To Toronto:		
Routing service	Route	002
	Use	Pool B
	External #	None
	Destination Code	6
	Absorb	None
	Normal route	002
Remote access	Rem access pkgs	01
	Line pool access	Pool M: ON
	Rem access pkgs	02
	Line pool access	Pool B: ON
	Line abilities	049
	Remote pkg	01
	Line abilities	050
	Remote pkg	02
Toronto office:		
Trunk/Line Data	Line 093	T1 E&M
	Answer Mode	Auto
	Line type	Pool N
	Line 300	Target line
	Received #	6221
Line Access	Set 6221	L300: Ring only
	Line pool access	Line pool N
To New York:		
Routing service	Route	001
	Use	Pool N
	External #	None
	Destination Code	4
	Absorb	None
	Normal route	001
To Santa Clara:		
Routing service	Destination Code	2
	Absorb	None
	Normal route	001

If a user in New York wishes to call Toronto within the network, they dial 6221. The local Enterprise Edge checks the number against the routing tables and routes the call according to the destination code 6, which places the call using Route 001.

The call appears on the auto answer line on the Enterprise Edge in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 002 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line received number. The call now alerts at telephone 6221 in Toronto.

Dialing plans with shared line pools

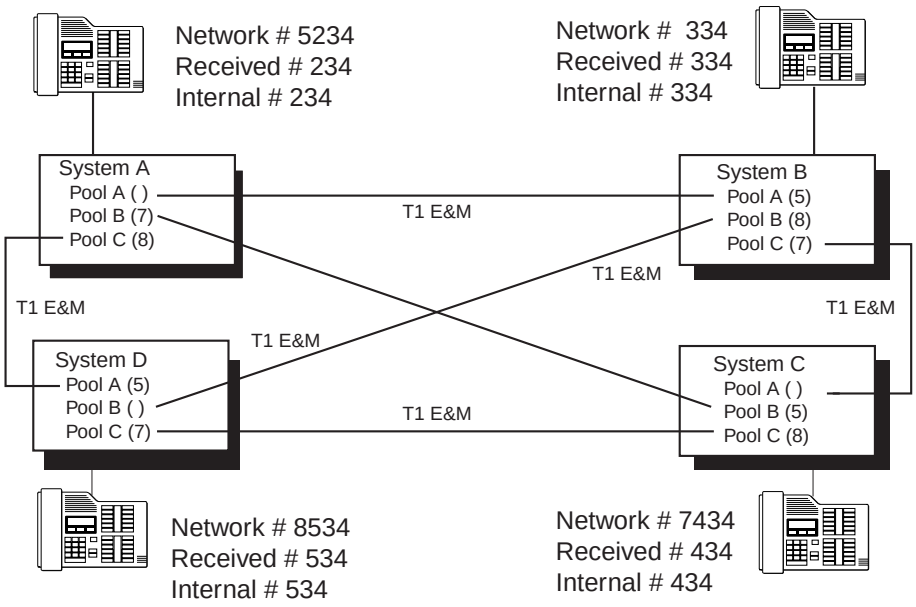
Using routes and destination codes is a powerful and efficient way to create a coordinated dialing plan. Line pools offer an alternate method of creating a dialing plan or supplementing the routing and destination codes.

If the Enterprise Edge systems are close to each other geographically, you can conserve resources by not duplicating access. For example, system A, B, and C are all within the same area code. System A has a line pool to Santa Clara, System B has a line pool to Montreal, and system C has a line pool to Miami. An Enterprise Edge user in system A can reach Miami by calling system C and using their line pool to Miami.

To simplify access between Enterprise Edge systems, all line pools that go to the same destination should have the same line pool access code. For example, system A and system B both have a line pool to Ottawa. You can configure both systems with the same line pool access code for the Ottawa line pool.

A dialing plan similar to the one in Network example using shared line pools. on page 340 will let you create a company directory that uses line pool access codes and unique DNs of a uniform length

Network example using shared line pools.



For instance, the person on system A at telephone 234 can press an Intercom button and dial 7434.

This means that telephone 234 has dialed the line pool access code of the trunk to system C, and will receive the dial tone of system C. The digits 434 then map to the Received number 434, and ring telephone 434 with an appearance of the associated target line.

Tips

Network calls that use routes are subject to any restriction filters that are in effect.

If the telephone used to make a network call has an appearance of a line used by the route, the call will move from the intercom button to the line button.

The telephone used to make a network call must have access to the line pool used by the route.

Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.

When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal set numbers.

Routes generally define the path between your Enterprise Edge switch and another switch in your network, not other individual telephones on that switch.

For dialing plan information with PRI, see Using a dialing plan to route outgoing PRI calls on page 137.

Networking examples

- PRI Networking with Meridian 1 on page 341
- PRI networking using Call-by-Call Services on page 346
- Enterprise Edge VoIP Gateway and M1 networking on page 348
- Toll bypass with Enterprise Edge VoIP Gateway on page 351
- Networking with QSIG (International systems only) on page 356
- Private networking with DPNSS (International systems only) on page 359

PRI Networking with Meridian 1

Some of the benefits of networking Enterprise Edge and Meridian M1 (version1.1) over PRI include

- common dialing plan
- centralized PSTN trunking (Enterprise Edge users can share the M1's PSTN trunks with M1 users)
- PRI networks can be used for voice, data, and video calls
- no usage costs when placing calls over private networks

Note: Private networking requires an Enterprise Edge PRI software keycode.

This example shows a private network composed of one central Meridian 1 (version 1.1), and two smaller sites with Enterprise Edge systems.

Note: Enterprise Edge systems only interact with M1 version 1.1. Enterprise Edge systems will no longer interact with the M1 version 2.0.

This could represent a large head office (with the Meridian 1) connected to several smaller branch offices. In this network, only the head office has trunks connected to the public network. The branch offices access the public network via the private connection to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing ‘9’, followed by the public number. For example, a user in the west end branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls are routed to the Meridian 1 by the Enterprise Edge routing table. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

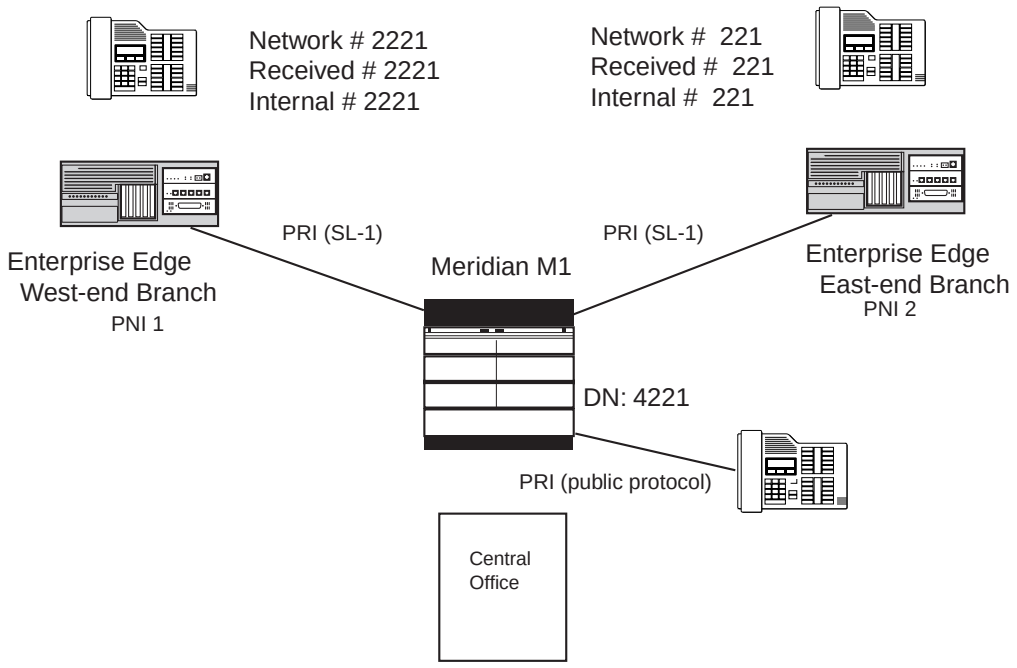
Note that the Private Network Identifier (PNI) is programmed at each end of the links. The PNI identifies the Enterprise Edge to the Meridian M1.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221. PRI networking with Meridian M1 (version 1.1) on page 343 illustrates this example. Refer to the following for hardware and routing programming for this network:

- PRI networking with Meridian M1 Routing information on page 343
- Hardware programming for the branch offices on page 343

In this example, there is additional configuration required as outlined in Additional Configuration to Enterprise Edge systems on page 345 and Guidelines to setting up PRI networking to Meridian M1 on page 345.

PRI networking with Meridian M1 (version 1.1)



Hardware programming for the branch offices

Heading	Parameter	Setting
West End office:		
Hardware programming	EE-DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary
East End office:		
Hardware programming	EE-DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary

PRI networking with Meridian M1 Routing information

Note: Private network routing information is highlighted in gray. Public network routing information is shown in white. In this example, the private DN length is 4 and the public DN length is 8. The public DN lengths depend on the market profile which you have downloaded.

Heading	Parameter	Setting
West End office:		
Trunk/Line Data	Line 245	Target line
	Received #	2221
Line Access	Set 2221	L245:Ring only
	Line pool access	Line pool PRI-A

Heading	Parameter	Setting
To Head Office: (call terminates on M1)		
Routing Service	Route	001
	Dial out #	No number
	Use	Pool PRI-A
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	0
To East End: (call terminates at East end)		
Routing Service	Destination Code	6
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	0
East End office:		
Trunk/Line Data	Line 245	Target line
	Received #	6221
Line Access	Set 6221	L245:Ring only
	Line pool access	Line pool PRI-A
To Head Office:(call terminates on M1)		
Routing Service	Route	001
	Dial out #	No number
	Use	Pool PRI-A
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	0
To West End: (Call terminates at West end)		
Routing Service	Destination Code	2
	Normal route	001
	Absorb	0
To Public Network: (Call terminates at M1)		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A

Heading	Parameter	Setting
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	0

Additional Configuration to Enterprise Edge systems

In this example, outgoing public network calls dialed from an Enterprise Edge set are passed to the Meridian M1, and the Meridian M1 is responsible for seizing a public trunk. For this reason, the ‘9’ prefix is left in the number passed to the Meridian 1.

This necessitates that the Public DN lengths table on each Enterprise Edge be modified to account for the extra leading digit. Essentially, the eight pre-configured entries are modified to include a leading ‘9’ in the prefix digits, and the length value for each entry is increased by one. The new entries are listed below. Note that regulatory requirements may demand an entry for 911. The Public DN lengths table is specific to individual market profiles.

Prefix	Length
Default	8
90	12
900	13
901	18
9011	19
91	12
9411	4
9911	4

Guidelines to setting up PRI networking to Meridian M1

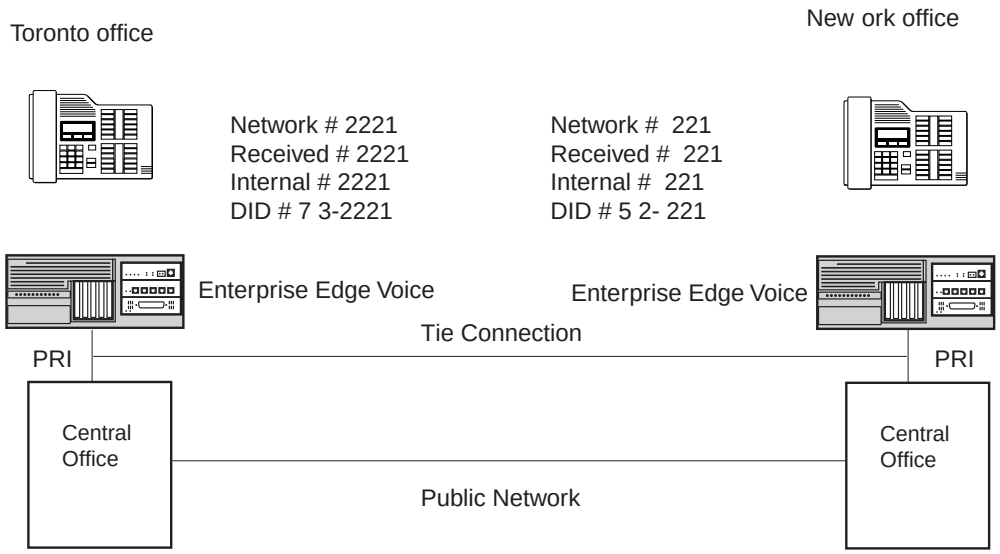
When setting up PRI networking with Meridian M1s, you must consider the following:

- Meridian M1 is the timing master for the private network PRI connections.
- Meridian M1 uses descending mode for PRI B-channel selection.
- The Meridian M1 must recognize calls dialed to 2xxx and 6xxx numbers, and route the call over PRI to either the East or West end offices. The same applies to incoming DID calls from the public network.
- The Meridian M1 must recognize numbers starting with ‘9’ as public numbers, whether the numbers are dialed by Meridian M1 users or by Enterprise Edge users.

PRI networking using Call-by-Call Services

This example highlights the use of PRI Call-by-Call Services. It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with an Enterprise Edge system and a PRI line. Each office has to handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office. To reduce long-distance costs, and to allow for a coordinated dialing plan between the offices, private lines are used to handle inter-office traffic.-

PRI networking using Call-byCall Services



If call-by-call services were *not* used, each Enterprise Edge system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic.
- 8 T1 E&M lines needed to handle inter-office calls.
- 8 lines needed to handle outgoing public calls

The total required is thus 28 lines. If the Enterprise Edge systems were using T1 trunks, then two T1 spans would be required at each office. Note that the total of 28 lines represents the worst case value for line usage. In reality, the total number of lines in use at any one time will generally be less than 28. For example, during periods of peak incoming call traffic, the demand for outgoing lines will be low.

With PRI call-by-call services, it is not necessary to configure a fixed allocation of trunks. Each of the 23 lines on the PRI can be used for DID, private Tie, or outgoing public calls. This consolidation means that it may be possible for each office to use a single PRI span, rather than two T1 spans. With PRI call-by-call services, the only limitation is that there are no more than 23 calls in progress at any one time.

The dialing plan at each Enterprise Edge site is configured to determine the call type based on the digits dialed by the user. If a user in Toronto wishes to dial a colleague in New York, they dial the 4-digit private DN (such as 6221). The dialing plan recognizes this as a private network DN, and routes the call using Tie service with a private numbering plan.

Incoming Tie calls are routed to sets based on the digits received by the network, which in this case will be the 4-digit private DN.

If a user in either location wishes to dial an external number, they dial '9', followed by the number (such as 9-555-1212). The dialing plan recognizes this as a public DN, and routes the call using Public service.

Incoming DID calls will be routed to sets based on the trailing portion of the digits received by the network. For example, if a public network user dials an employee in the Toronto office, the network will deliver digits 4167632221. Enterprise Edge will route the call using the last four digits, 2221.

PRI Call-by-Call Services Routing Information

Note: Private network routing information is highlighted in gray. Public network information is shown in white.

Heading	Parameter	Setting
Toronto office:		
Hardware	EE-DTM	PRI
	Protocol	NI-2
Trunk/Line Data	Line 245	Target line
	Received #	2221
Line Access	Set 2221	L245:Ring only
	Line pool access	Line pool PRI-A
To New York:		
Routing Service	Route	001
	External #	No number
	Use	Pool PRI-A
	Service type	Tie
	ServiceID	1
	DN type	Private
	Destination Code	6
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	Service type	Public

Heading	Parameter	Setting
	Destination Code	9
	Normal route	002
	Absorb	ALL
New York office:		
Hardware	EE-DTM	PRI
	Protocol	NI-2
Trunk/Line Data	Line 245	Target line
	Received #	6221
Line Access	Set 6221	L245:Ring only
	Line pool access	Line pool PRI-A
To Toronto:		
Routing Service	Route	001
	External #	No number
	Use	Pool PRI-A
	ServiceType	Tie
	ServiceID	1
	DN type	Private
	Destination Code	2
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	Service type	Public
	Destination Code	9
	Normal route	002
	Absorb	ALL

Enterprise Edge VoIP Gateway and M1 networking

This example shows a private network composed of one central Meridian 1, and two smaller sites with Enterprise Edge systems connected over IP trunks through a corporate IP network. This could represent a large head office (with the Meridian 1) connected to several smaller branch offices.

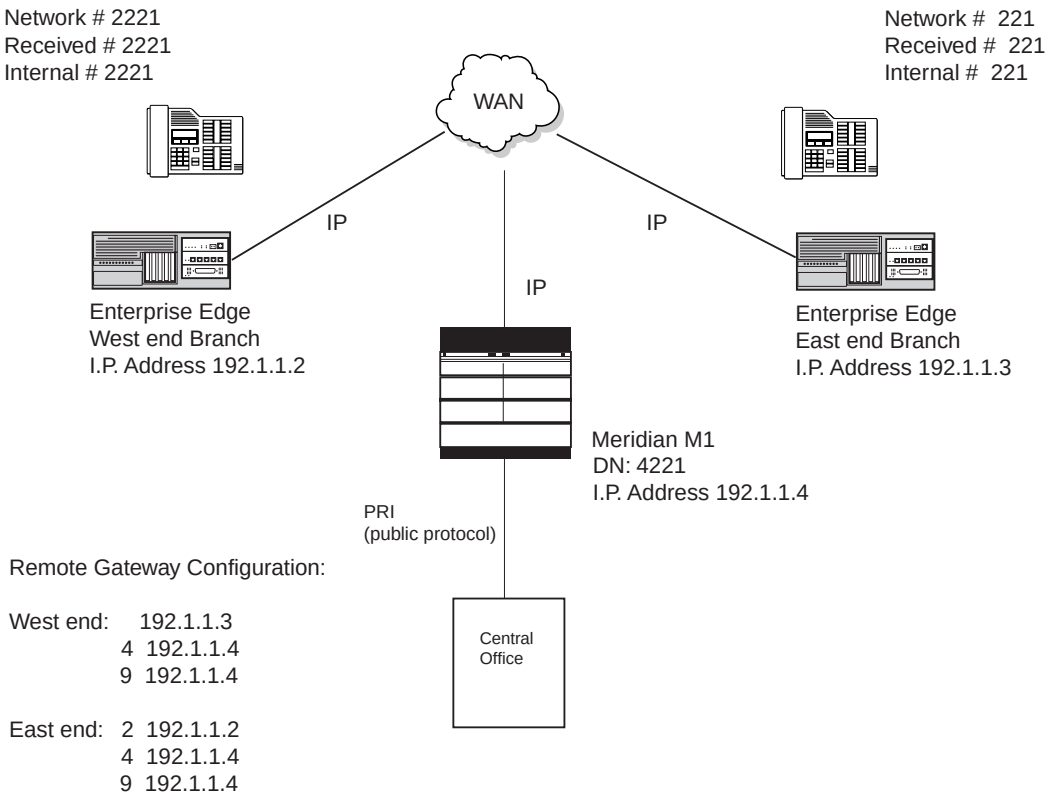
In this network, only the head office has trunks connected to the public network. The branch offices access the public network using IP trunks to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing ‘9’, followed by the public number. For example, a user in the west end branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls are routed to the Meridian 1 by the Enterprise Edge routing table. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221.

Note: The quality of the IP trunk connection is assessed during initial call setup, and if the quality is poor, Enterprise Edge will try to find an alternate route to complete the call based on the fallback programming definitions in the routing table. For simplicity, this example does not show programming for fallback. Therefore, in this example, if the quality of the IP connection is low during the call setup phase, the call will be maintained at that quality. For an example of fallback programming, see Toll bypass with Enterprise Edge VoIP Gateway on page 351.

Note: Enterprise Edge VoIP Gateway requires a software keycode.

VoIP Gateway and M1 Networking



The Call Managers examine the Called Party Number digits and route the call to the corresponding IP address.

VoIP and M1 Networking Routing information

In the table that follows, private network routing information is highlighted in gray. Public network routing information is shown in white.

Heading	Parameter	Setting
West End office:		
Trunk/Line Data	Line 241	Target line
	Received #	2221
Line Access	Set 2221	L241:Ring only
	Line pool access	Line pool A
To Head office (M1):		
Service/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	None
To East End:		
Service/Routing Service	Destination Code	6
	Normal route	001
	Absorb	None
To Public Network:		
Service/Routing Service	Route	002
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	None
East End office:		
Trunk/Line Data	Line 241	Target line
	Received #	6221
Line Access	Set 6221	L241:Ring only
	Line pool access	Line pool A
To Head Office: (M1)		
Service/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	None

Heading	Parameter	Setting
To West End:		
Service/Routing Service	Destination Code	2
	Normal route	001
	Absorb	None
To Public Network:		
Service/Routing Service	Route	002
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	None

In this example, outgoing public network calls dialed from an Enterprise Edge set are passed to the Meridian M1, and the Meridian M1 is responsible for seizing a public trunk. For this reason, the “9” prefix is left in the number passed to the Meridian 1.

Note: Ensure that Line Pool A is used for IP trunks.

Guidelines to setting up Meridian M1 in this example

In order for the digit counting algorithm for outgoing IP calls to take into account this extra digit, the Private Network Access Code must be set to “9” on each Enterprise Edge system.

The Meridian M1 must recognize incoming 2xxx and 6xxx DID calls, and route the call over IP trunks to either the East or West end offices.

The Meridian M1 must recognize numbers starting with “9” as public numbers, whether the numbers are dialed by Meridian M1 users or by Enterprise Edge users.

Toll bypass with Enterprise Edge VoIP Gateway

This example shows a private network composed of one Enterprise Edge system in Toronto and one Enterprise Edge system in Ottawa, connected over IP trunks through a corporate IP network.

In this network, each Enterprise Edge system has a PRI trunk to the Central Office, and IP trunks to the other Enterprise Edge system. Calls from the Toronto system to the Ottawa system and the Ottawa public network are made over IP trunks with fallback to the PRI trunks when IP trunks are congested. This configuration allows for cost savings by using the corporate IP network whenever possible, thereby bypassing toll charges that would be incurred by using the public network.

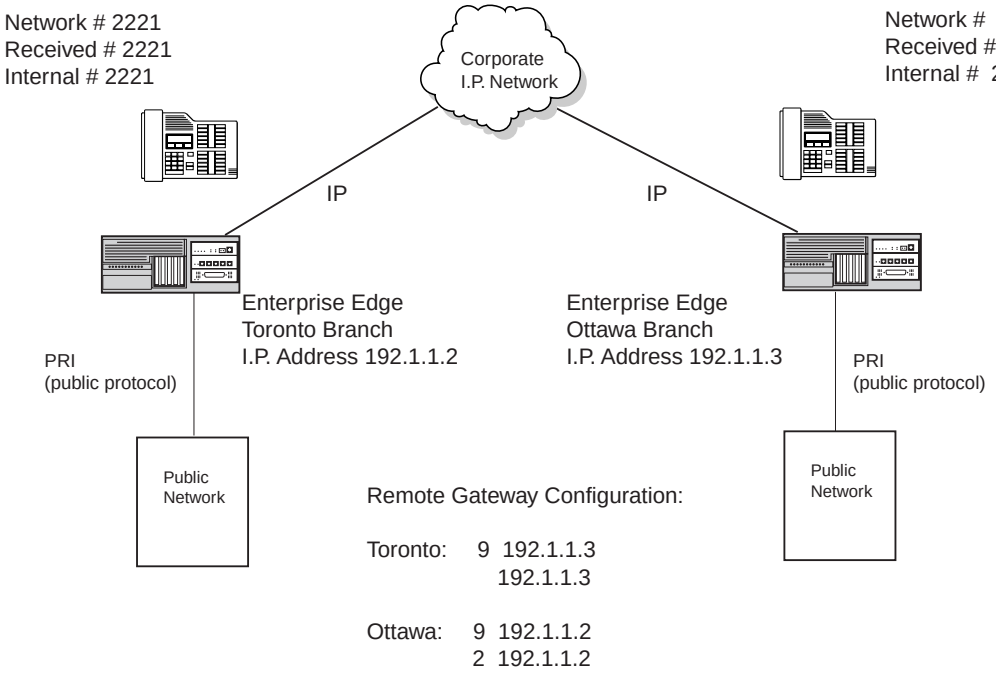
Note: When a call gets rerouted over the PSTN due to congestion, the user may see a prompt "Expensive route." The warning indicates that toll charges may be applied to this call.

Users at both locations access the public network by dialing "9", followed by the public number. For example, a user in Toronto might dial 9-555-1212 (for a local call), or 9-1-613-555-1212 (for a long distance call to Ottawa). Local calls would be sent directly to the Central Office over PRI trunks. Long distance calls to Ottawa would be sent over IP trunks; the Ottawa system would tandem these calls to the local Central Office over PRI trunks.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in Toronto wants to call a user in Ottawa within the private network, they dial 6221.

Note: Enterprise Edge VoIP Gateway requires a software keycode.

Toll bypass with Enterprise Edge VoIP Gateway



The Call Manager at the Toronto office examines the Called Party Number digits and determines that it should be routed to the IP address corresponding to the Ottawa office. The Ottawa office receives the call, sees that the leading digit(s) match its Private Network Access Code, and uses a destination code to route the call over its public trunks to the PSTN.

This is a simplified example where only calls to the 613 Area Code are routed by the Ottawa node. In a real world configuration, it would also be desirable to handle Area Codes that are 'close', for example Montreal: 514.

Toll bypass with Enterprise Edge VoIP Gateway Routing Information

Note: Private network routing information is highlighted in gray.

Heading	Parameter	Setting
Toronto office:		
Lines/Trunk/Line Data	Line 241	Target line
	Received #	2221
Terminals & sets/Line Access	Set 221	L241:Ring only
	Line pool access	Line pool A Line pool PRI-A
Calls to Ottawa office:		
Services/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
Services/Routing Service	Route	002
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Private
Services/Routing Service	Destination Code	6
	Schedule 4	001
	Absorb	None
	Normal route	002
	Absorb	None
Calls to Ottawa Public Network:		
Services/Routing Service	Route	003
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Route	004
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Public
	Destination Code	91613
	Normal route	004
	Absorb	1
	Schedule 4	003
	Absorb	None

Heading	Parameter	Setting
To Public Network:		
Services/Routing Service	Destination Code	9161A
	Normal route	004
	Absorb	1
	Destination Code	916A
	Normal route	004
	Absorb	1
	Destination Code	91A
	Normal route	004
	Absorb	1
	Destination Code	9A
	Normal route	004
	Absorb	1
Ottawa office:		
Trunk/Line Data	Line 241	Target line
	Received #	6221
Line Access	Set 6221	L241:Ring only
	Line pool access	Line pool A Line pool PRI-A
To Toronto office:		
Services/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Route	002
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Private
	Destination Code	2
	Normal route	002
	Absorb	None
	Schedule 4	001
	Absorb	None

Heading	Parameter	Setting
To Toronto Public Network:		
Services/Routing Service	Route	003
	Use	Pool A
	External #	(leave blank)
	DN type	Public
Services/Routing Service	Route	004
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Public
	Destination Code	91416
	Normal route	004
	Absorb	1
	Schedule 4	003
	Absorb	None
To Public Network:		
Services/Routing Service	Destination Code	9141A
	Normal route	004
	Absorb	1
	Destination Code	914A
	Normal route	004
	Absorb	1
	Destination Code	91A
	Normal route	004
	Absorb	1
	Destination Code	9A
	Normal route	004
	Absorb	1

The implications on the configuration on each node are:

- each node must have the Private Network Access Code set to the value 9.
- each node must have destination code(s) that match the Private Network Access Code plus digits corresponding to calls terminating in the local PSTN. For example, if the Private Network Access Code is ‘9’, the node in Ottawa would require a destination code of ‘91613’. Similarly, Toronto would require the following destination code: 91416.

Note: Ensure that Line Pool A is used for IP trunks.

To allow for fallback to PRI trunks when the IP trunks are congested, you must also program the following Routing service settings:

- Set the start and end times for Sched 4 to 1:00 so that IP calls can be made 24 hours a day.

- Program the Sched 4 Service setting to Auto and enable overflow routing by changing the Overflow setting to Y (Yes).
- A control set must be defined for all sets on the system that make calls over IP trunks. See Control set on page 92 for more information.

You must program Remote Packages so that the IP trunks in Pool A can access the lines in Pool PRI-A in a toll bypass scenario. In other words, you must give package 01 access to pool PRI-A and you must assign package 01 to all IP trunks. For more information, see Remote access packages on page 160.

Networking with QSIG (International systems only)

QSIG is an ETSI standard signalling for multi-vendor peer-to-peer communications between PBXs and/or central offices.

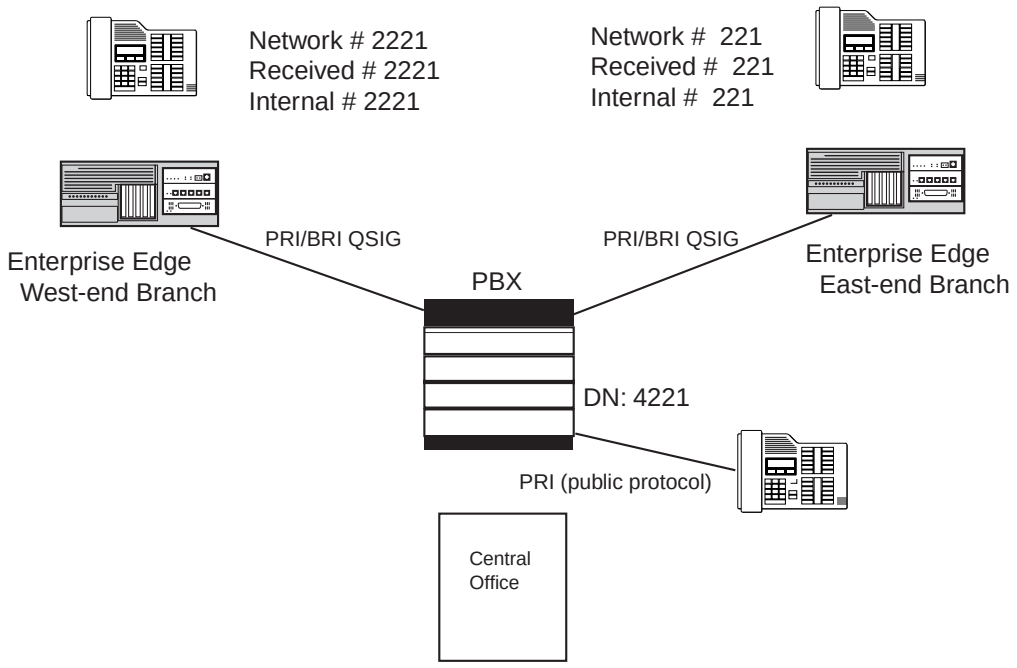
This networking example shows a private network composed of one central PBX, and two smaller sites with Enterprise Edge systems. This could represent a large head office connected to several smaller branch offices. In this network, only the head office has trunks connected to the public network. The branch offices access the public network via the private connection to the head office.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221. In this example, the private DN length is 4 and the public DN length is 8. The public DN lengths depend on the market profile which you have downloaded.

QSIG networking on page 357 illustrates this example. Refer to the following for hardware and routing programming:

- Hardware programming for the branch offices on page 357
- Routing information for QSIG network example on page 358

QSIG networking



Hardware programming for the branch offices

The following table lists the settings for some of the hardware parameters. Note that in this example:

- Private DN length is 4 and the public DN length is 8. The public DN lengths depend on the market profile which you have downloaded.
- B channel sequencing for BRI is hard coded as descending. B channel sequencing for PRI can be programmed. If it is programmed ascending on one of the branch Enterprise Edge servers, it must be programmed descending at the opposite end on the PBX.

Heading	Parameter	Setting
West End office:		
Hardware programming	EE-DTM/EE-BRIM	PRI/BRI
	Protocol	QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary
East End office:		
Hardware programming	EE-DTM/EE-BRIM	PRI/BRI
	Protocol	QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

Routing information for QSIG network example

Note: Private network routing information is highlighted in gray.

Heading	Parameter	Setting
West End office:		
Trunk/Line Data	Line 245	Target line
	Received #	2221
Line Access	Set 2221	L245:Ring only
	Line pool access	Line pool PRI-A
To Head Office: (call terminates on M1)		
Routing Service	Route	001
	Dial out #	No number
	Use	Pool PRI-A
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	0
To East End: (call terminates at East end)		
Routing Service	Destination Code	6
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	Dial out #	No number
	Use	Pool PRI-A
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	0
East End office:		
Trunk/Line Data	Line 245	Target line
	Received #	6221
Line Access	Set 6221	L245:Ring only
	Line pool access	Line pool PRI-A
To Head Office:		
Routing Service	Route	001
	Dial out #	No number
	Use	Pool PRI-A
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	0

Heading	Parameter	Setting
To West End: (Call terminates at West end)		
Routing Service	Destination Code	2
	Normal route	001
	Absorb	0
To Public Network: (Call terminates at M1)		
Routing Service	Route	002
	Dial out #	No number
	Use	Pool PRI-A
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	0

Private networking with DPNSS (International systems only)

DPNSS supports the Universal Dialling Plan (UDP), an international standard for sending and receiving private numbers over networks. The UDP requires that a number include the following:

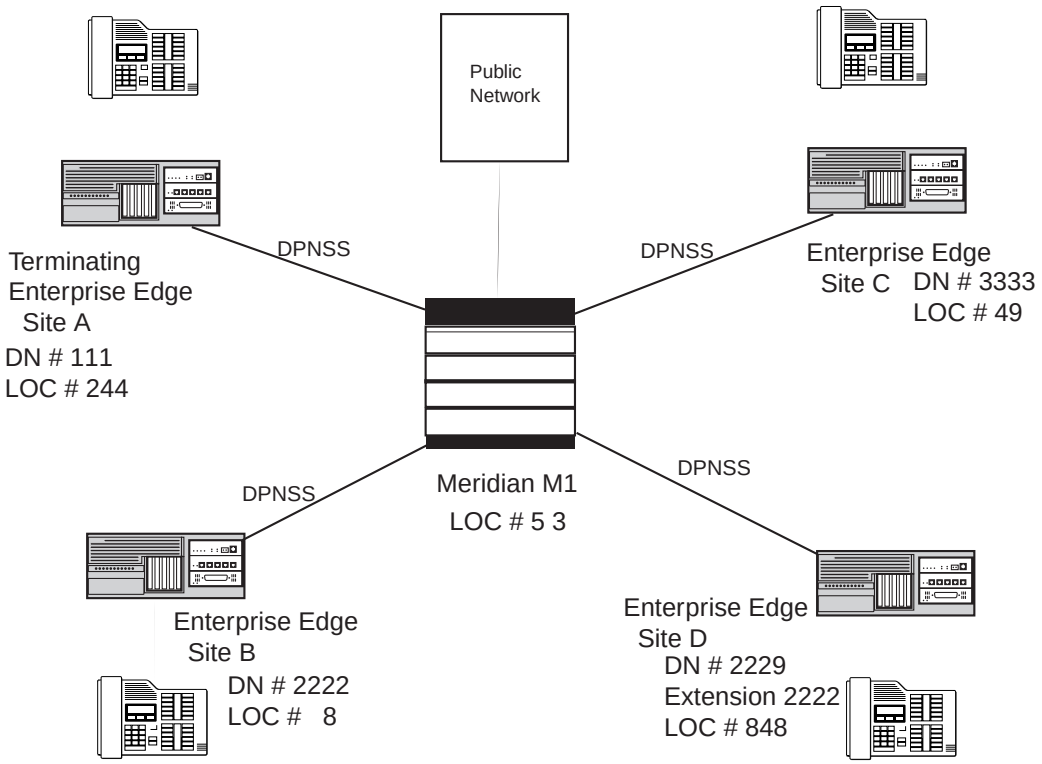
- a Home Location Code (HLC) which is assigned to a PBX as part of it's destination code and can be any string of digits up to a maximum length of seven. For each HLC, a routing code must be programmed in the system.
- a Directory Number (DN) which is assigned to individual extensions as a line appearance. The DN appears as the last string segment in a dialed number. In the number 244-1111, "1111" is the DN.
- a Private Access Code which can be programmed into the system as part of the destination (dest) code table to prevent conflicts with the internal numbering system.

A typical Private Number, using a Private Access Code and dialed from another site on the network, is show below.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+ 848	+ 2222	= 6-848-2222

In this networking example, a private network is formed when several systems are connected through a Meridian M1 and a terminating Enterprise Edge system. Each site has its own HLC and a range of DNs. DPNSS networking on page 360 illustrates this example. For information on programming routing for this example, refer to Routing information for DPNSS network example on page 361.

DPNSS networking



Calls are dialed and identified to the system as follows:

- To reach a set inside the Private Network, at the Enterprise Edge site, the user dials the DN of choice.
- To reach a set inside the Private Network, but on another site, the user dials an HLC + DN.
- To reach a set outside the Private Network, the user dials an Access Code + HLC + DN

  Each node has its own destination (dest) codes to route the call appropriately.

The following table shows examples of the construction of numbers used when dialling within the example network. Note that 6 is the Private Access code.

Dialling examples within a DPNSS Private Network

Calling Site	LOC/HLC	Calling Party Number	Called Site	Dialling String	Called Party Number
Site A	244	244 1111	Site B	6 668 2222	668 2222
Site B	668	668 2222	Site D	6 848 2222	848 2222
Site D	848	2222	Site D	2229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Routing information for DPNSS network example

Heading	Parameter	Setting
Private Network: (for each branch Enterprise Edge)		
Routing Service	Route	001
	Dial out #	No number
	Use	Pool N
	DN type	none (private access code 6 is programmed)
	Destination Code	6
	Normal route	001
	Absorb	1
Public Network:		
Routing Service	Route	002
	Dial out #	No number
	Use	Pool N
	DN type	public
	Destination Code	9
	Normal route	002
	Absorb	1

For more information on creating a private numbering plan with DPNSS, refer to

- Guidelines for creating a private numbering plan with DPNSS on page 361
- Customizing the routing service on page 362

Guidelines for creating a private numbering plan with DPNSS

Use the following guidelines when creating a private numbering plan with DPNSS.

- When creating HLCs for the nodes in your system, avoid numbering conflicts between network nodes and internal DNs, Hunt Group DNs.
- Program a Private Access Code into your dest routing tables to avoid conflicts with your internal HLC and dest code numbering plan. For example, if a dialout HLC is 848, but this number already exists in the Norstar system for an extension, the routing tables should add a Private Access Code to the dest code. If the code is programmed as “6”, the dest code becomes 6848. 6848 uses a route to dial out 888 using the DPNSS line pool, allowing the call to be placed.

  Note that a Private Access Codes is required only for specific DPNSS features such as Diversion, Route Optimization, and Redirection.

Customizing the routing service

You can customize the routing service using the following restrictions:

- Direct Inward Access (DIA) lines allow incoming calls on private circuits to be directed to telephones without going through the normal call reception. Each DIA line is assigned to one or more extensions and is given a distinct Private Received number. When someone on another system on the network dials the Private Received number on a DPNSS line, the Enterprise Edge system checks all received digits, compares the digits to an internal table and routes the call to the appropriate DIA line. All extensions programmed to have access to that DIA line will then alert for the incoming call.
- Dialling restrictions can be added to lines in line pools. Filters can restrict the use of the line to specific area codes.
- Host system signaling codes can be part of the dial out for a route. Routing can also be used as an alternate method for a direct-dial number. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1. Because overflow routing directs calls using alternate line pools, a call may be affected by different line restrictions when it is handled by overflow routing.

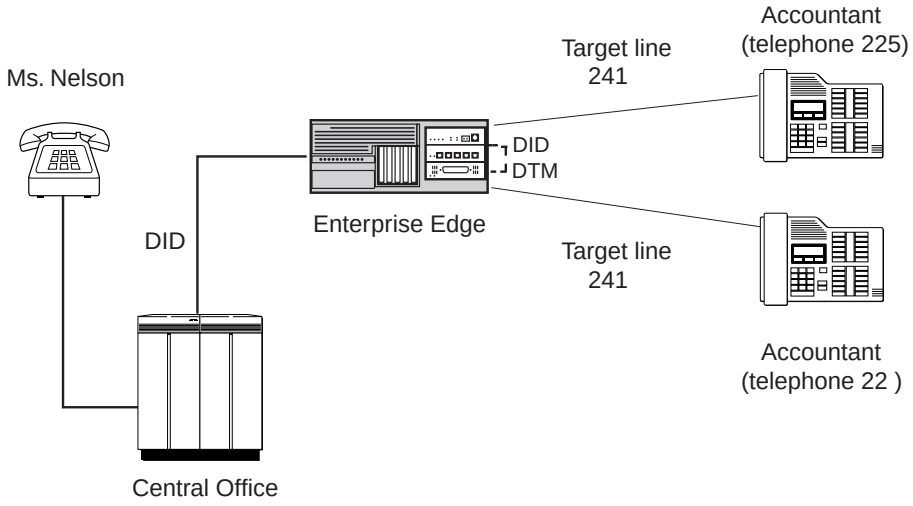
Public networking scenarios

The following scenarios illustrate various Enterprise Edge calls you can make with public networking:

- Call one or more Enterprise Edge telephones on page 363
- Call Enterprise Edge and select tie lines to a private network on page 363
- Call Enterprise Edge and select lines to the public network on page 364

Call one or more Enterprise Edge telephones

Ms. Nelson is a bank customer who has a question for an accountant. She dials the telephone number 555-4321 that maps onto target line 241. All of the accountants' telephones ring.

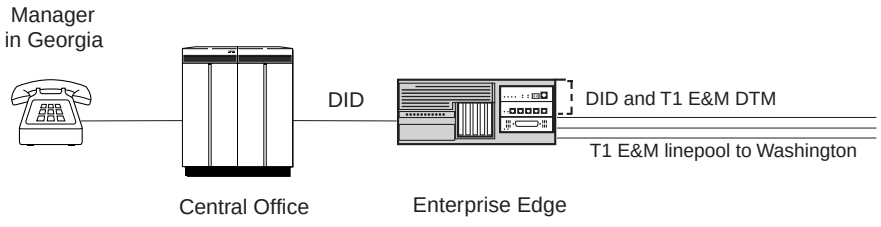


Hardware: Enterprise Edge, an EE-DTM with lines programmed as DID.

Heading	Parameter	Setting
Trunk/Line Data	Received # Line 061	4321 (for Line 241) T1 DID
Rec'd # length	Received # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)

Call Enterprise Edge and select tie lines to a private network

A manager in Georgia wants to use the tie lines at headquarters to call Washington. He dials a telephone number 555-5321 that maps onto the DISA DN, enters a Class of Service (COS) password, then dials a line pool access code to select a tie line to Washington.

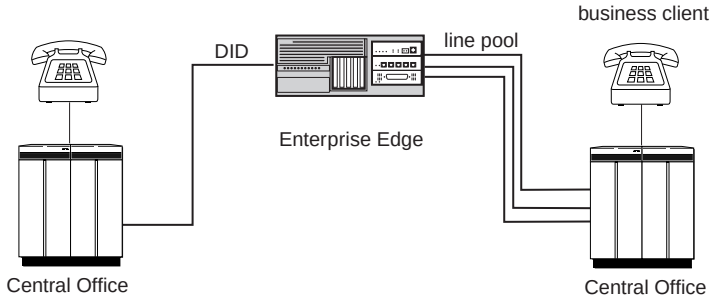


Hardware: Enterprise Edge, an EE-DTM with one T1 DID line and three T1 E&M lines.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 061	T1 DID
Access codes	DISA DN	5321
Rec'd # length	Rec'd # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)
Outgoing trunk: Trunk/Line Data	Line 062 Line type	T1 E&M Pool F
Access codes	Line pool F	6 (up to 4 digits)
COS pswds		Define restrictions. Define remote access pkgs. Assign a restriction filter to the line. Assign COS passwords and filters for each Class of Service.

Call Enterprise Edge and select lines to the public network

Gord is working from home, and needs to make a long-distance business call from home. To avoid being charged, he dials the telephone number 555-4321 that maps onto the Auto DN at work. After hearing the dial tone, Gord dials a line pool access code 1234 to select a line to the public network. He then dials the long-distance number.



Hardware: Enterprise Edge, EE-DTM with several T1 DID lines.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 061	T1 DID
Access codes	Auto DN	4321
Rec'd # length	Rec'd # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)

Heading	Parameter	Setting
Lines /Restrictions and Remote access		Define restriction filters. Define remote access packages. Assign a remote restriction and remote package to the line.
Outgoing trunk: Trunk/Line Data	 Line 001 Line type	 Loop Pool A
Access codes	Line pool A	1234
Lines /Restrictions		Assign a restriction filter to the line.

Private networking scenarios

Note: The ability to perform private networking is only available with Enterprise Edge software keycodes.

The following scenarios illustrate various Enterprise Edge calls you can make with private networking:

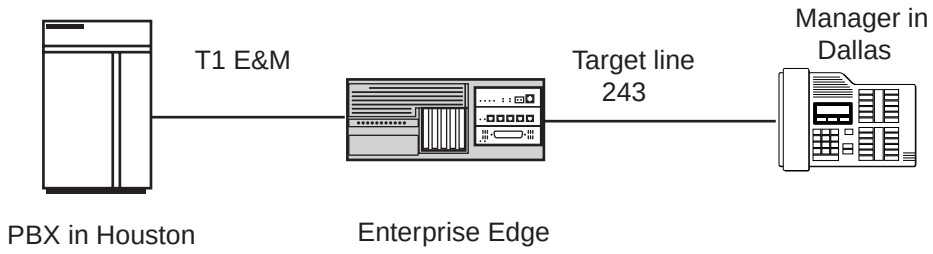
- Call one or more Enterprise Edge telephones on page 363
- Call Enterprise Edge and select tie lines to a private network on page 363
- Call Enterprise Edge and select lines to the public network on page 364
- Call one or more Enterprise Edge telephones on page 366
- Call Enterprise Edge and select tie lines to other nodes in the private network on page 366
- Call Enterprise Edge and select lines to the public network on page 367
- Select T1 E&M trunks to the private network on page 368
- Using Enterprise Edge Line Redirection on page 368

Refer to the following for information on programming DID:

- PRI dialing plan example for 2-way DID on page 370
- PRI DID and 2-way DID on page 370

Call one or more Enterprise Edge telephones

The production supervisor in Houston selects the less expensive company tie line to call the manager at the Administration office in Dallas. Once the line is selected, the production supervisor dials the digits that will map onto the target line of the manager in Dallas.

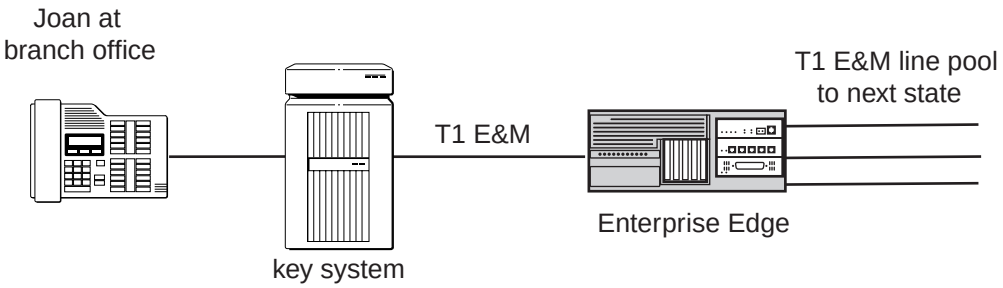


Hardware: Enterprise Edge, an EE-DTM with a T1 E&M line.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	 Received # Line 061 Answer Mode	 4321(for target line 243) T1 E&M Auto
Rec'd # length	Received # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)

Call Enterprise Edge and select tie lines to other nodes in the private network

At a branch office, Joan selects a tie line to the main office downtown. After hearing the dial tone, she dials a line pool access code to select another tie line to a branch office in the next state.



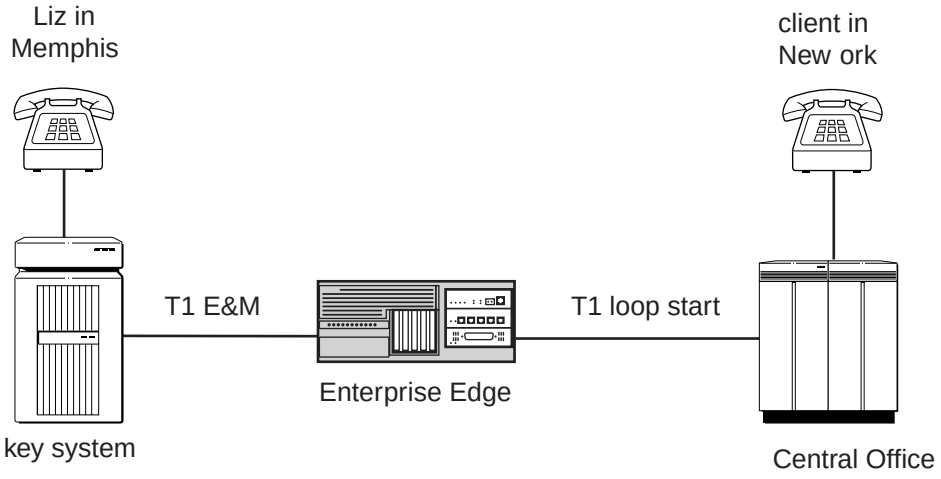
Hardware: Enterprise Edge, an EE-DTM with four T1 E&M lines (3 lines in the line pool and 1 incoming line).

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	 Line 061 Answer mode	 T1 E&M Auto

Heading	Parameter	Setting
Under Lines /Restrictions and Remote access		Define restriction filters. Define remote access packages. Assign a remote restriction and remote package to the trunk.
Outgoing trunk: Trunk/Line Data	 Line 062 Line type	 T1 E&M Pool D
Access codes	Line pool D	71 (can be from 1 to 4 digits)
Lines /Restrictions		Assign a restriction filter to the trunk.

Call Enterprise Edge and select lines to the public network

In Memphis, Liz needs to call long-distance to a client in New York. She selects a tie-line to the branch office in New York. After hearing the dial tone, she dials a line pool access code to select a line to the public network. Then, she dials the client's number as a local call.

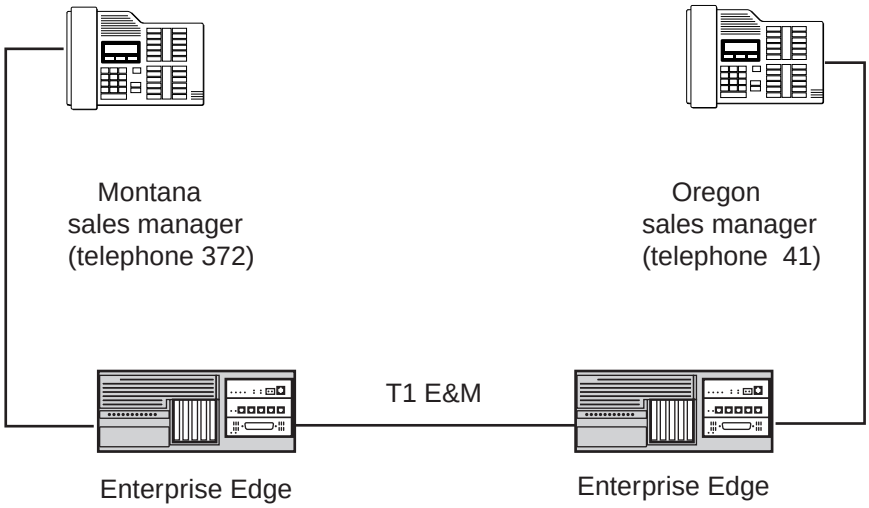


Hardware: Enterprise Edge, an EE-DTM with a T1 E&M line.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 091 Answer mode	T1 E&M Auto
Under Lines /Restrictions and Remote access		Define restriction filters and remote access packages. Assign a remote restriction and remote package to the trunk.
Outgoing trunk: Trunk/Line Data	 Line 061 Line type	 Loop Pool B
Access codes	Line pool B	73 (can be 1 to 4 digits)
Lines /Restrictions		Assign a restriction filter to the line.

Select T1 E&M trunks to the private network

For a confidential call, the Montana sales manager presses the line button for a private E&M trunk to the Oregon office. This automatically alerts at the line appearance on the telephone of the Oregon sales manager.



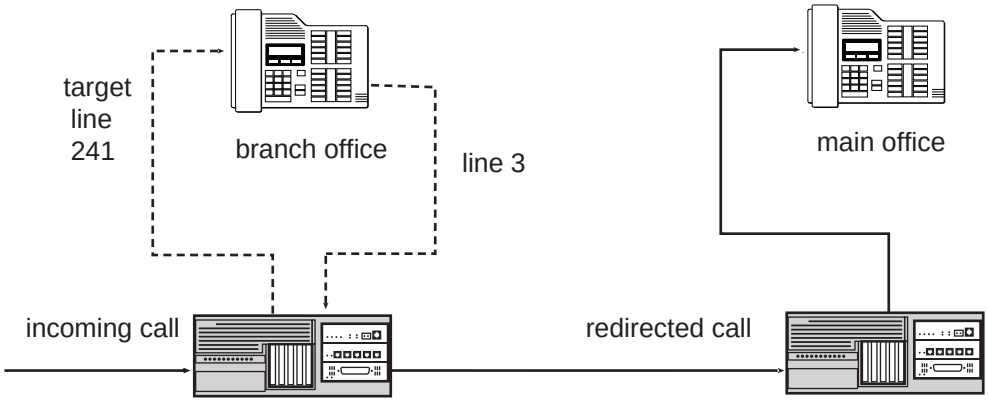
Hardware: (for both systems) Enterprise Edge, an EE-DTM with a T1 E&M line.

Heading	Parameter	Setting
Montana: *Outgoing trunk:* Trunk Data (Line 049) Line Data (Line 049)	 Line Line type	 T1 E&M Private to 372
Oregon: *Incoming trunk:* Trunk Data (Line 057)	 Line Answer mode Line type	 T1 E&M Manual Private to 641

Using Enterprise Edge Line Redirection

The branch office is receiving more calls than it can handle, so it redirects one of its lines to the main office. All calls that come in on target line 241 will be routed out on line 003 to the main office. Whenever a call is redirected, the target line and outgoing line will be busy for the duration of the call.

The branch office only routes out one call at a time on the redirected line. If the target line is busy, the next incoming call will go to the prime set and not be redirected.



Hardware: Enterprise Edge, an EE-DTM with one T1 E&M line or one T1 DID line.

Tips

Any line appearance on a telephone can be selected as the incoming line to be redirected. Restriction filter restrictions on the line are checked against the filter in effect at the time a call is redirected not when redirection is programmed.

A target line can not be selected as the outgoing line for redirection. The incoming trunk must have disconnect supervision.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 061: T1 Loop Trunk mode: Super Answer mode: Auto OR Line 065: T1 DID OR Line 065: T1 E&M Answer mode: Auto Received #: 4321 (for target line 232)	Incoming trunk: Trunk/Line Data
Rec'd # length	Received # length: 4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)	Rec'd # length
Outgoing trunk: Trunk/Line Data	Line 062: T1 Loop OR Line 066: T1 E&M	Outgoing trunk: Trunk/Line Data
Capabilities	Allow redirect: Y	Capabilities

PRI dialing plan example for 2-way DID

The following list shows the general steps involved in configuring a dialing plan for two-way DID using a Public service. In this example the user dials the prefix 8 to place a call over a PRI line.

1. Choose **Resources**, **Telephony**, **Hardware** and configure the DTI (EE-DTM) for PRI.
2. Select **Public** as the protocol.
3. For incoming calls, program target lines to match the DID digit that is being received on the PRI interface.
4. Set **Dial Out** to **None**.
5. Select **PRI-A** as the line pool.
6. Set **ServiceType** to **Public**.
7. Choose **Services, Routing Service** to enter a Destination Code (8 in this example).
8. Set **Absorb Length** to **All**.
9. Provide access to the PRI Pool for the set that you are dialing out from. This is programmed in **Terminals & Sets**.
10. Define received digits for target lines.
11. Define limits for incoming and outgoing public calls, see Programming Call by Call service selection on page 168.

Note: 2-way DID does not have to be configured for Call-by-call service.

PRI DID and 2-way DID

When configuring PRI DID with 2-way service, the channels programmed as DID at the CO must be the lowest B-channels on PRI. On your Enterprise Edge system, the BchanSeq mode must be set to **descending**. In this configuration, all calls on PRI must be Public service.

For example, channels 1 to 4 are configured as DID at the CO. The CO uses **ascending** mode for B-channel selection, and Enterprise Edge uses **descending** mode.

Appendix B: ISDN Overview

This chapter provides the following information:

- Welcome to ISDN
- Services and features for ISDN BRI and PRI
- ISDN hardware
- ISDN standards compatibility
- Planning your ISDN network
- ISDN programming

Welcome to ISDN

Integrated Services Digital Network (ISDN) technology provides a fast, accurate and reliable means of sending and receiving voice, data, images, text, and other information through the telecom network.

ISDN uses existing analog telephone wires and divides it into separate digital channels which increases bandwidth.

ISDN uses a single transport to carry multiple information types. What once required separate networks for voice, data, images, or video conferencing is now combined onto one common high-speed transport.

Nortel endeavours to test all variations of ISDN PRI on Enterprise Edge; however, due to the number of variations, this is not always possible.

Analog versus ISDN

ISDN offers significantly higher bandwidth and speed than analog transmission because of its end-to-end digital connectivity on all transmission circuits. Being digital allows ISDN lines to provide better quality signaling than analog POTS lines, and ISDN out-of band data channel signaling offers faster call set up and tear down.

While an analog line carries only a single transmission at a time, an ISDN line can carry one or more voice, data, fax, and video transmissions simultaneously.

An analog modem operating at 14.4 K takes about 4.5 minutes to transfer a 1MB data file and a 28.8K modem takes about half that time. Using one channel of an ISDN line, the transfer time is reduced to only 1 minute and if two ISDN channels are used, transfer time is just 30 seconds.

When transmitting data, the connect time for an average ISDN call is about 3 seconds per call, compared to about 21 seconds for the average analog modem call.

Types of ISDN service

Two types of ISDN services (lines) are available: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Each line is made up of separate channels known as B and D channels which transmit information simultaneously.

- BRI is known as “2B+D” because it consists of 2 B-channels and 1 D-channel.
- PRI is known as “23B+D”(in North America) or as “30B+D” (in Europe). In North America, “23B+D” consists of 23 B-channels and 1 D-channel (T1 carrier). In Europe, “30B+D” consists of 30 B-channels and 1 D-channel (E1 carrier).

B channels

B channels are the bearer channel and are used to carry voice or data information and have speeds of 64 kbps. Since each ISDN link (BRI or PRI) has more than one B-channel, a user can perform more than one transmission at the same time using a single ISDN link.

D channels

The standard signaling protocol is transmitted over a dedicated data channel called the D-channel. The D-channel carries call setup and feature activation information to the destination and has speeds of 16 kbps (BRI) and 64 kbps PRI. Data information consists of control and signal information and for BRI only, packet-switched data such as credit card verification.

ISDN layers

ISDN layers refer to the standards established to guide the manufacturers of ISDN equipment and are based on the OSI (Open Systems Interconnection) model. The layers include both physical connections, such as wiring, and logical connections, which are programmed in computer software.

When equipment is designed to the ISDN standard for one of the layers, it works with equipment for the layers above and below it. There are three layers at work in ISDN for Enterprise Edge. To support ISDN service, all three layers must be working properly.

- Layer 1: A physical connection that supports fundamental signaling passed between the ISDN network (your service provider) and the Enterprise Edge system.When the LED on a BRI S/T Media Bay Module configured as BRI is lit, your layer 1 is functioning.
- Layer 2: A logical connection between the central office or the far end and the Enterprise Edge system.Enterprise Edge has one or two of these connections for each BRI link, and one for each PRI link. Without Layer 2, call processing is not possible and there is no dial tone.
- Layer 3: Also a logical connection between the ISDN network (your service provider) and the Enterprise Edge system. For BRI lines, layer 3 is where call

processing and service profile identifier (SPID) information is exchanged. This controls which central office services are available to the connection. For example, a network connection can be programmed to carry data calls.

Note: Throughout this chapter, references are made to Service profile identifiers (SPIDs). SPIDs are a part of the BRI National ISDN standard. SPIDs are not used in the ETSI BRI standard or on PRI.

The system of layers is important when you are installing, maintaining, and troubleshooting an ISDN system. For information about troubleshooting ISDN, see Troubleshooting your Enterprise Edge system on page 305.

ISDN Bearer capability

Bearer capability describes the transmission standard used by theBRI or PRI line so that it can work within a larger ISDN hardware and software network.

The bearer capability for BRI and PRI is voice/speech, 3.1 kHz audio, and data (unrestricted 64 kbps, restricted 64 kbps, or 56 kbps).

Services and features for ISDN BRI and PRI

As part of an ISDN digital network, your system supports enhanced capabilities and features, including:

- faster call set up and tear down
- high quality voice transmission
- dial-up Internet and local area network (LAN) access
- video transmission
- network name display
- name and number blocking (PRI, BRI and analog)
- access to public protocols

PRI services and features

- Call-by-call service selection (NI protocol)
- coordinated dialing plan (SL1 protocol)
- Emergency 911 dialing, internal extension number transmission
- access to Meridian 1 private networking (SL-1 protocol)

BRI services and features

- data transmission at speeds up to 128 kbps per loop (depending on the bandwidth supported by your service provider)
- shared digital lines for voice and data ISDN terminal equipment

Enterprise Edge Basic Rate Interface (BRI) cards also support D-channel packet service between a network and terminal connection. This allows you to add applications such as point-of-sale terminals without additional network connections.

Any analog or digital network connections can be shared by all Enterprise Edge telephones, peripherals and applications, and ISDN terminal equipment (TE).

Enterprise Edge supports the following ISDN services and features offered by ISDN service providers:

- D-channel packet service (BRI only) to support devices such as transaction terminals. Transaction terminals are used to "swipe" credit or debit cards and transmit the information to a financial institution in data packets.
- calling number identification (appears on both Enterprise Edge sets and ISDN terminal equipment with the capability to show the information)
- Multi-Line Hunt or DN Hunting which switches a call to another ISDN line if the line usually used by the Network DN is busy. (*BRI only*)
- subaddressing of terminal equipment (TE) on the same BRI loop. However, terminal equipment which supports sub-addressing is not commonly available in North America.(*BRI only*)

Transmission of B-channel packet data using nailed up trunks is not supported by Enterprise Edge.

Contact your ISDN service provider for more information about these services and features. For more information about ordering ISDN service in North America, see Ordering ISDN PRI on page 381 and Ordering ISDN BRI on page 381.

The terminal equipment (TE) connected to the Enterprise Edge system can use some feature codes supported by the ISDN service provider. See "ISDN services and features" in the *Enterprise Edge Telephone Feature Programming Guide* for more information.

Network name display

This feature allows ISDN to deliver the Name information of the users to those who are involved in a call that is on a public or private network. For information about programming this feature, see Network Name Display on page 163.

Your Enterprise Edge system displays the name of an incoming call when it is available from the service provider. If the Calling Party Name has the status of "private" it may be displayed as "Private name" if that is how the service provider has indicated that it should be displayed. If the Calling Party Name is unavailable it may be displayed as "Unknown name".

Your system might display the name of the called party on an outgoing call, if it is provided by your service provider. Your system sends the Business Name concatenated with the set name on an outgoing call but only after the Business Name has been programmed.

The available features include:

- Receiving Connected Name
- Receiving Calling Name
- Receiving Redirected Name
- Sending Connected Name
- Sending Calling Party Name

For more information, see Network Name Display on page 163. Consult your customer service representative to determine which of these features is compatible with your service provider.

Name and number blocking (North America only)

When activated, Feature 8 1 9 allows you to block the outgoing name and/or number on a per-call basis. Name and number blocking can be used with an Enterprise Edge set. For information about programming this feature, see Outgoing name and number blocking (ONN) on page 165.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Call by Call service selection for PRI (NI protocol)

PRI lines can be dynamically allocated to different service types with the Call by Call feature. PRI lines do not have to be pre-allocated to a given service type. Outgoing calls are routed through a dedicated PRI Pool and the calls can be routed based on various schedules.

The service types that may be available, depending on your service provider are described below.

Public

Public service calls connect your Enterprise Edge set with a Central Office (CO). DID and DOD calls are supported.

Private

Private service calls connect your Enterprise Edge set with a Virtual Private Network. DID and DOD calls are supported. A private dialing plan may be used.

Tie

Tie services are private incoming and outgoing services that connect Private Branch Exchanges (PBX) such as Enterprise Edge.

FX (Foreign Exchange)

FX service calls logically connect your Enterprise Edge set to a remote CO. It provides the equivalent of local service at the distant exchange.

Outwats

Outwats is for outgoing calls. This allows you to originate calls to telephones in a specific geographical area called a zone or band. Typically a flat monthly fee is charged for this service.

Inwats

Inwats is a type of long distance service which allows you to receive calls originating within specified areas without a charge to the caller. A toll-free number is assigned to allow for reversed billing.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Emergency 911 dialing

The ISDN PRI feature is capable of transmitting the telephone number and internal extension number of a calling station dialing 911 to the Public Switched Telephone Network. State and local requirements for support of Emergency 911 dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations. For most installations the following configuration rules should be followed, unless local regulations require a modification.

- All PSTN connections must be over PRI
- In order for all sets to be reached from a Public Safety Answering Position (PSAP), the system must be configured for DID access to all sets. In order to reduce confusion, the dial digits for each set should be configured to correspond to the set's extension number
- The OLI digits for each set should be identical to the DID dialed digits for the set
- The routing table should route "911" to a PRI line pool
- If attendant notification is required, the routing table must be set up for all 911 calls to use a dedicated line which has an appearance on the attendant's console
- The actual digit string "911" is not hard-coded into the system. More than one emergency number can be supported

If transmission of internal extension numbers is not required or desired, then it is recommended that the person in charge of the system maintain a site map or location directory that allows emergency personnel to rapidly locate an Enterprise Edge set given its DID number. This list should be kept up to date and readily available.

2-way DID

With PRI the same lines can be used for receiving direct inward dialing (DID) and for making direct outward dialing (DOD) calls.

The dialing plan configured by your customer service representative determines how calls are routed. Consult your customer service representative to determine whether or not this feature is compatible with your service provider.

Dialing Plan and PRI

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing incoming and outgoing calls. All PRI calls must go through a dialing plan.

The Dialing Plan

- allows incoming calls to be routed to sets based on service type and digits received
- provides the ability to map user-dialed digits to a service type on a Call by Call basis
- allows long distance carrier selection through user-dialed Carrier Access Codes

Consult your customer service representative to determine how your dialing plan is configured.

ISDN hardware

To support connections to an ISDN network and ISDN terminal equipment, your Enterprise Edge must be equipped with a BRI S/T Media Bay Module (EE-BRIM S/T) or a Digital Trunk Media Bay Module (EE-DTM) card configured for PRI.

PRI hardware

The Digital Trunk Media Bay Module (EE-DTM) is configured for PRI. In most PRI network configurations, you need one EE-DTM configured as PRI to act as the primary clock reference. The only time when you may not have an EE-DTM designated as the PRI primary clock reference is in a network where your Enterprise Edge system is connected back-to-back with another switch using a PRI link. If the other switch is loop-timed to your Enterprise Edge system, your EE-DTM (PRI) can be designated as a timing master.

If your Enterprise Edge has more than one EE-DTM configured as PRI, you must assign the first EE-DTM as the primary reference, the second EE-DTM as the secondary reference, and the third EE-DTM as the timing master.

BRI hardware

The loops on the EE-BRIM S/T module can be programmed to support either network or terminal connections. This allows you to customize your arrangement of lines, voice terminals, data terminals and other ISDN equipment. This section describes some basic hardware configurations for network and terminal connections for each loop type.

Detailed wiring information for BRI and PRI network and terminal connections is included in the *Enterprise Edge Installation and Maintenance Guide*.

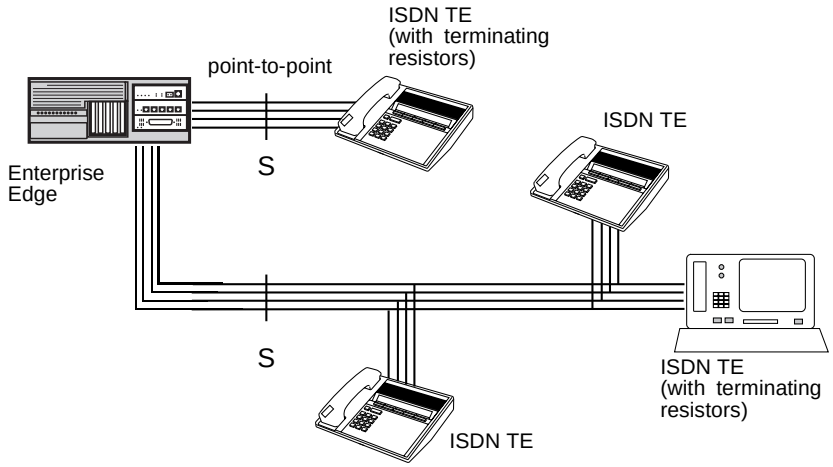
An EE-BRIM S/T provides four loops. Each loop can be individually programmed as:

- an S reference point connection (S loop) to ISDN terminal equipment (TE), or
- a T or S reference point connection (T loop or S loop) to an ISDN network using an external NT1

S reference point

The S reference point connection provides either a point-to-point or point-to-multipoint digital connection between Enterprise Edge and ISDN terminal equipment (TE) that uses an S interface.

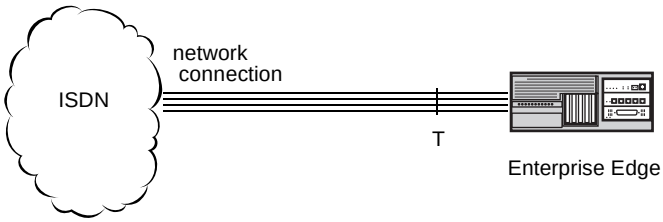
S loops support up to seven ISDN DNs, which identify TE to the Enterprise Edge system.



T reference points

The T reference point connections provide a point-to-point digital connection between the ISDN network and Enterprise Edge.

A T loop provides lines that can be shared by all Enterprise Edge telephones, peripherals and applications, and ISDN TE.



A T loop can be used in combination with an S loop to provide D-packet service for a point-of-sale terminal adapter (POSTA) or other D-packet device. D-packet service is a 16 kbps data transmission service that uses the D-channel of an ISDN line.

To deliver D-packet service, a network connection (T loop) is programmed to work with a terminal connection (S loop). The loops must be on the same physical module.

Clock Source for ISDN

Systems with ISDN interfaces need to synchronize clocking with the ISDN network and any ISDN terminal equipment connected to the network. Systems synchronize clocking to the first functionally available network connection. If there are excessive errors on the reference network connection, the next available network connection is used for clock synchronization. The clock synchronization process generates alarm codes and event messages. Clock synchronization is supported by the Digital Trunk Media Bay Module, BRI S/T Media Bay Module and the Fiber Expansion Media Bay Module.

The Enterprise Edge derives timing from the network using T reference points (loops). Terminal equipment on S reference points (loops) derive timing from the Enterprise Edge system.

When you configure the network connections to the Enterprise Edge, you should take into account the system preferences for selecting loops for synchronization:

- lower numbered loops have preference over higher numbered loops
- the loop preference order is: 201, 202, 203, 204 etc.
- the system skips S and analog loops on Mod2 Card 1, when selecting a network connection for synchronization

Systems with only S loops act as timing masters for the attached terminal equipment (TE), and are not synchronized to the network. ISDN TE without access to a network connection (BRI lines) has limited or no functionality.

If your system has both an EE-BRIM S/T configured as BRI, and an EE-DTM configured as PRI, it is recommended that you use PRI as the primary clock source. See PRI hardware on page 377.

Other ISDN BRI equipment

NT1

The NT1 (network termination type 1) connects an S interface (four-wire) to a U interface (two-wire). In most cases, it connects loops from an EE-BRIM S/T module to the network connection, which uses the Uinterface .

The NT1 converts and reformats data so it can be transmitted to and from the S or T connection. In addition, it manages the maintenance messages travelling between the network and the NT1, and between the NT1 and the Enterprise Edge system.

The NT1 from Nortel Networks is packaged two ways:

- a stand alone package which contains one NT1 card (NTBX80XX) and a power supply (NTBX81XX)
- a modular package which contains up to 12 NT1 cards (NTBX83XX) and a power supply (NTBX86AA)

ISDN standards compatibility

In North America, Enterprise Edge ISDN equipment supports National ISDN standards for basic call and calling line identification services. Enterprise Edge BRI is compliant with National ISDN-1 and PRI is compliant with National ISDN-2.

Enterprise Edge does not support EKTS (Electronic Key Telephone System) or CACH (Call Appearance Call Handling).

In Europe, Enterprise Edge supports ETSI Euro and QSIG standards, and PRI SL-1 protocol.

Planning your ISDN network

Consult the *Enterprise Edge Installation and Maintenance Gui*de to determine a configuration of ISDN trunks and terminal equipment (TE) for the Enterprise Edge system, then order the appropriate ISDN capability package from your ISDN service provider.

For ISDN BRI service your service provider supplies service profile identifiers (SPIDs), network directory numbers (Network DNs), terminal endpoint identifiers (TEIs), and other information as required to program your Enterprise Edge, TE and other ISDN equipment.

Enterprise Edge does not support any package with EKTS (Electronic Key Telephone System) or CACH (Call Appearance Call Handling). EKTS is a package of features provided by the service provider and may include features such as Call Forwarding, Link, Three-Way Calling, and Calling Party Identification.

Ordering ISDN PRI

Ordering ISDN PRI service in Canada

In Canada, order Megalink™ service, the trade name for standard PRI service and set the Enterprise Edge equipment to the supported protocol that is identified by your service provider, either DMS-100 or NI-2.

Ordering ISDN PRI service in United States

In the United States order PRI service from your service provider. Set the Enterprise Edge equipment to the PRI protocol indicated by your service provider.

Ordering ISDN PRI service outside of Canada and the United States

Outside of Canada and the United States order Euro ISDN PRI and/or BRI service from your service provider. Set the Enterprise Edge equipment to the Euro ISDN protocol.

Ordering ISDN BRI

Ordering service ISDN BRI service in Canada

In Canada, order Microlink™ service, the trade name for standard BRI service. You can order either regular Microlink™ service, which includes the CLID (Calling Line Identification) feature, or Centrex Microlink™, which includes access to additional ISDN network features (including Call Forwarding).

When ordering Microlink™ service, it must be ordered with EKTS (Electronic Key Telephone System) turned off. If you will be using a point-of-sale terminal adapter (POSTA), ask for D-packet service to be enabled.

Ordering ISDN BRI service in the United States

In the U.S., regardless of the CO (Central Office) type, order National ISDN BRI-NI-1 with EKTS (Electronic Key Telephone System) turned off. Use the following packages as a guideline for ordering your National ISDN BRI-NI-1. However, we recommend using packages M or P with the Enterprise Edge system. Contact your service provider for more information about the capability packages it offers. Bellcore/National ISDN Users Forum (NIUF ISDN packages supported by Enterprise Edge (for ordering in U.S.)

	Capability	Feature set	Optional features	Point-of-sale	Voice	Data
M	Alternate voice/circuit-switched data on both B-channels	--	calling line identification	--	✓	✓
P	Alternate voice/circuit-switched data on both B-channels D-channel packet	flexible calling for voice (not supported by Enterprise Edge) Basic D-Channel Packet	additional call offering (not supported by Enterprise Edge) calling line identification	✓	✓	✓

If you want to transmit both voice and data, and support D-channel packet service, order package P. However, Enterprise Edge does not support the flexible calling for voice and additional call offering features that are included in package P.

Multi-Line Hunt may be ordered with your package. When a telephone number (the Network DN) in the group of numbers assigned by your service providers is busy, the Multi-Line Hunt feature connects the call to another telephone number in the group. Enterprise Edge supports the feature only on point-to-point, network connections (T loop). Check with your service provider for more information about Multi-Line Hunt.

Any of the ISDN packages will allow you to use sub-addressing, but your ISDN TE must be equipped to use sub-addressing for the feature to work.

Ordering ISDN BRI service outside of Canada and the United States

Outside of Canada and the United States order Euro ISDN PRI and/or BRI service from your service provider. Set the Enterprise Edge equipment to the Euro ISDN protocol.

Supported ISDN protocols

The switch used by your service provider must be running the appropriate protocol software and the correct version of that software to support ISDN PRI and BRI. Each protocol is different and supports different services. Contact your service provider to make sure that your ISDN connection has the protocol you require.

For more information on the supported protocols and services, refer to Call by Call service selection for PRI on page 166.

ISDN programming

Most of the programming for PRI and BRI lines, and ISDN terminals is done under the Media Bay Modules heading. This section gives you an overview of programming for PRI and BRI lines, ISDN terminals and devices, and D-packet services.

PRI or BRI programming activity	Programming heading
View or change the Digital Trunk Media Bay Module (EE-DTM) Configure EE-DTM for PRI	Resources, Media Bay Modules
Provision or pre-provision lines	Resources, Media Bay Modules, Bus 0#, Modules on Bus, Module 1, Provision lines
Enable or disable BRIM-S/T and EE-DTM	Resources, Media Bay Modules, Bus 0#, Modules on Bus Module 1
View status of line, loop or port	Resources, Media Bay Modules, Bus #, Ports on Bus

Program PRI resources

Some steps may not be necessary depending on the service you are using. For more detailed programming information, see Media Bay Modules on page 69 and Maintenance on page 259. For complete module installation instructions and safety precautions, see the *Enterprise Edge Installation and Maintenance Guide*.

1. Collect the information supplied by your service provider to support your ISDN package.

2. Install the EE-DTM. (For information, refer to the *Enterprise Edge Installation and Maintenance Guide*.)

3. Configure the EE-DTM for PRI. For information on how to configure a module, see Module on page 72.

4. Configure the lines on the modules. For more information, see Lines on page 108.

Programming ISDN BRI resources

Some steps may not be necessary depending on the service you are providing. For more detailed programming information, see Media Bay Modules on page 69 and Maintenance on page 259. For complete module installation instructions and safety precautions, see the *Enterprise Edge Installation and Maintenance Guide*.

1. Collect the information supplied by your service provider to support your ISDN package. This includes network service profile identifiers (SPIDs) and Network DNs. If you are supporting a point-of-sale terminal adapter, you also need one or more static terminal endpoint identifiers (TEIs).

2. Install the EE-BRIM S/T module in the Enterprise Edge system. (For information, refer to the *Enterprise Edge Installation and Maintenance*).

3. Select the module type (BRI-ST). For information on selecting a module type, *Guides* Module on page 72.

4. Select the type (T or S) for each loop. For information on how to select a loop type, see Loops on page 121.

5. If the module uses a T loop, enter the following configuration information (for North America only) as supplied by your service provider: the SPID assigned to the loop, the number of B-channels associated with each SPID, the Network DNs used with the network SPID, and the call type of the Network DN. Repeat the programming for the second network SPID, if any.

   If the T loop is used for D-packet service: turn on the service, assign the appropriate S-loop mapping and assign the static TEIs (provided by the telco to support a point-of-sale terminal adapter or other D-packet service device) to the loop.

   If the loop type is S, select the sampling used on the loop. Assign ISDN DNs to the loop and designate one of the assigned ISDN DNs to be the DN for the loop (Loop DN).

   Note: You can have a maximum of 28 ISDN DNs on your system. The default ISDN DN range is 501-528.

6. Provision the loops and lines. For more information, see Provision lines on page 81.

7. If you are configuring auto-answer BRI trunks to map to target lines, program the received number for the target line (see Setting Received number on page 117) to be the same as the Network DN supplied by your service provider.

   From the **Terminals & Sets**, **Line Access** heading, assign the ISDN lines and target lines to the appropriate ISDN DNs (the set of DNs reserved for use by ISDN devices). ISDN lines can also be assigned to the DNs used by Enterprise Edge telephones or any other devices connected to the Enterprise Edge system.

   Program the ISDN terminals and devices with the appropriate ISDN DNs and terminal SPIDs by following the instructions that come with the devices. For more information see Program ISDN equipment on page 386. If you are setting up a D-packet service, program the point-of-sale terminal adapter or other D-packet service device with the appropriate TEI (provided by your service provider), terminal SPID, and DN by following the instructions that come with the device.

Program PRI lines

When the hardware configuration is complete, your PRI lines are ready to be programmed. For information on programming your PRI lines, see Call by Call service selection for PRI on page 166.

Program ISDN BRI lines (North America)

When the hardware configuration is complete, your BRI lines are ready to be programmed in the same way as analog lines. You can, for example, place them in pools and assign them to Enterprise Edge sets and ISDN terminal equipment. However, there are some differences in the way BRI lines work that will influence how you configure them to handle incoming and outgoing calls.

For BRI lines, in most cases, your service provider supplies two SPIDs – one for each B channel. Each SPID and one or more Network DNs are associated with a single line. Calls to a Network DN come in on a specific line, and pressing a line button selects the same line every time.

If your service provider supplies you with a single SPID for both B channels, incoming and outgoing calls are handled according to the loop. The two lines provided by the BRI loop are “pooled” for both incoming and outgoing calls.

For example, if Loop 201is programmed with a single SPID, which supports lines 061 and 062, incoming calls made to a Network DN associated with the SPID appear on either line 061 or line 062. If you press the line button for line 061, either line 061 or line 062 is selected. For loops which use a single SPID, assign both lines on a loop to a set to guarantee that all calls appear at the set.

Program Direct Inward System Access (DISA) on PRI lines (North America)

When an EE-DTM is configured for PRI, all lines on that module are set to Auto Answer without Direct Inward System Access (DISA). DISA can however be accessed by one of two methods.

Method 1:

Define the DISA DN to match the trailing digits of the Called Party Number (CDN).

With Public, Private, and Tie service types, the CDN is simply truncated to the Target Line Receive Digit Length and is parsed to match the Target Line Receive Digits. DISA can be accessed by having the DISA DN match the trailing digits of the CDN. For example, with a Receive Digit Length = 4, and DISA DN = 1234, a call made to Public DN 763-1234 will be handled as follows:

- the ISDN setup message will contain a CDN of 763-1234
- the CDN will be truncated to the 4 digits, 1234
- 1234 matches the DISA DN
- the call will be answered with DISA

Method 2:

Use incoming Call by Call (CbC) Service routing to map the call type to the DISA DN. Refer to Call Routing on page 128 for more information.

With FX, INWATS, 900, and SDS service types, either a Service Id (SID) or a CDN is mapped to Target Line Receive Digits. This is programmed under Call by Call Service routing on page 130. DISA may be accessed by having the SID or CDN map to the DISA DN. This example has a Receive Digit Length = 4,
DISA DN = 1234, and CbC Routing with (Service Type = FX, Map from SID = 2, Map to digits = 1234).

A call presented to the Enterprise Edge system with service type FX and SID 2 will be handled as follows:

- The ISDN setup message will specify FX with SID = 2
- The FX SID = 2 will be mapped to DISA DN digits 1234

The call will be answered with DISA.

Program ISDN equipment

PRI modules support various applications that are enabled by PRI. For a list of the type of applications that are supported, refer to the*Enterprise Edge Feature Programming Telephone Guide*.

Terminal equipment for BRI cards

ISDN devices and terminals connected to the Enterprise Edge system must be configured under Services, Telephony Services, Loops. You choose directory numbers for ISDN equipment from a pre-determined range of DNs (501-528). Any of the ISDN DNs can be assigned to an S loop but each can only be assigned to one loop and a single device.

Devices on an S loop (BRI cards only)

Terminal equipment using an S loop must be assigned an ISDN directory number (ISDN DN). This allows the TE to be assigned lines and to communicate with other devices connected to the Enterprise Edge system. Each DN can be assigned to only one TE and one loop.

You assign ISDN DNs to S loops from the **Telephony Services** subheading, under **Loops**, **DNs on Loop**, **Assign DNs**. Each S loop can be programmed with eight ISDN DNs, but you cannot exceed a total of 28 ISDN DNs for the Enterprise Edge system.

Loop DN (North America)

Once you have assigned ISDN DNs to a loop, designate one of the DNs as a Loop DN. The Loop DN acts as a main ISDN DN and completes the configuration of the loop.

The ISDN terminal equipment (TE) on the loop is also programmed with its ISDN DN. See the instructions that come with the ISDN device for information about how to program it to recognize its assigned DN. Most devices will require both a terminal service profile identifier (terminal SPID) and a DN, and some will require two terminal SPIDs and two ISDN DNs. The SPID used with the device should not be confused with a SPID used for network connections using a T loop.

To create a terminal SPID for a device, add at least two zeros to the end of the of the ISDN DN. Add more zeros to the beginning or end of the ISDN DN until you have the length of SPID required by the TE. For example, if an ISDN telephone requires a six-digit SPID and has a DN of 667, its SPID is 066700. If the same TE requires a minimum of ten digits, the SPID is 0000066700.

Most ISDN terminals require a five-digit SPID. An ISDN PC card usually requires a ten-digit SPID. Follow the directions that come with the ISDN device to program it with a SPID and ISDN DN.

D-packet service (BRI only)

The D-packet service supplied by the Enterprise Edge system supports a point-of-sale terminal adapter (POSTA). Connecting a POSTA allows transaction terminals (devices where you "swipe" credit or debit cards) to transmit information using the D channel of the BRI line, while the B channels of the BRI line remain available for voice and data calls. A special adapter links transaction equipment (such as cash registers, credit card verification rigs, and point-of-sale terminals) to the X.25 network, a data communications network designed to transmit information in the form of small data packets.

To support the D-packet service, your ISDN network and financial institution must be equipped with a D-packet handler. To convert the protocol used by the transaction equipment to the X.25 protocol, your ISDN network must also be equipped with an integrated X.25 PAD which works with the following versions of X.25: Datapac 32011, CCITT, T3POS, ITT and API. The ISDN service package you order must include D-packet service (for example, Package P in the United States; Microlink™ with D-channel in Canada).

Your service provider supplies a Terminal Endpoint Identifier (TEI) and DN to support D-packet service. The TEI is a number between 00 and 63 (in Canada, the default range is 21-63). Your service provider may also supply you with a DN to program your D-packet device. The DN for D-packet service becomes part of the dialing string used by the D-packet to call the packet handler.

POSTA for ISDN BRI

When you configure D-channel packet service, you are specifying the transmission path between an ISDN loop on the network side of the Enterprise Edge system and the ISDN loop on the set side (the loop used by the point-of-sale terminal adapter). The service is turned on and configured from the **Services**, **Telephony Services, Loops** subheading (S or T loop for EE-BRIM S/T modules).

To set up D-packet service:

1. Go to the programming settings for the network loop (T, or NT loop) under **Services**, **Telephony Services**, **Loops**

2. Select the loop type used by POSTA: **S** loop or **LT** loop.

3. Enter the terminal endpoint identifiers (TEIs) supplied by your service provider.

4. Select “D-packet enabled” to Y.

Appendix C: Setting Up Remote Routers

This appendix includes information on setting up Nortel Networks routers and how to set up a range of UDP as a high priority.

This appendix includes:

- Creating an Outbound Traffic Filter
- Sample Criteria, Ranges, and Actions for UDP Filtering

Creating an Outbound Traffic Filter

To create an outbound traffic filter:

1. In the Configuration Manager window, click **Circuits** and then click **Edit Circuits**.
   The Circuit List window appears.

2. Select a circuit.

3. Click the **Edit** button.
   The Circuit Definition screen appears with the circuit you selected highlighted.

4. Click **Protocols**, click **Edit Protocol Priority,** and then click **Priority/Outbound Filters**.
   The Priority/Outbound Filters window appears.

5. Click **Template**.
   The Filter Template Management window appears.

6. Click **Create**.
   The Create Priority/Outbound Template window appears.

7. Type a descriptive name in the Filter Name field.

8. Click **Criteria**, click **Add**, click **Datalink**, click **IP,** and then click **Criterion**.
   The Add Range window appears. If you choose the User-Defined criterion, the Add User-Defined Field window appears first.

9. Type a minimum and maximum value to specify the range, and then click the **OK** button.
   The Add Range window closes. The new criterion and ranges now appear in the Filter Information field of the Create Priority/Outbound Template window.

10. Click **Action**, click **Add** and then click **action**.

11. Click the **OK** button.
    The Filter Template Management window opens. The new template appears in the templates list.

12. Click **Done**.
    The Priority/Outbound Filters window opens.

13. Click **Create**.
    The Create Filter window opens.

14. Select a circuit in the Interfaces field.

15. Select a template in the Templates field.

16. Type a descriptive name in the Filter Name field.

17. Click **OK**.
    The Priority/Outbound Filters window opens.

18. Click **Apply**.
    The filter is applied to the circuit.

Sample Criteria, Ranges, and Actions for UDP Filtering

The filtering goal is to place all VoIP H.323 traffic leaving a particular interface in the high priority queue. From the BayRS Site Manager:

Use a criteria path of **Criteria**, **Add**, **IP**, **IP**, **UDP Destination Port**

The range is 2065 to 2067.

The action path is: **Action**, **IP**, **Add**, **High Queue**.

Note: This example shows how to give H.323 traffic priority over other protocols on the interface.

Appendix D: Market profile attributes

Market profiles are selected by the user at system startup. Each market profile is designed using a set of system defaults that provide specific functionality for the region in which the system is deployed. Enterprise Edge offers a choice of the following market profiles:

- Global
- United Kingdom
- Sweden
- Holland
- CALA (Central American Latin American)
- Caribbean
- North American
- Denmark

For more information on selecting Market Profiles, refer to *Enterprise Edge Installation and Maintenance Guide*.

For information on the functionality associated with each market profile, refer to:

- Languages available to customer on page 391
- System defaults on page 392

Languages available to customer

The following table lists the languages available for each market profile and a list of some countries that will be using each profile.

Market profile	Language	Sample of countries using this profile
Global	English, French, Spanish, Turkish	Turkey, India, Saudi Arabia
United Kingdom	British, VIOC	England, Ireland
Sweden	English, Swedish	Sweden
Holland	English, Dutch	Holland
CALA	English, French, Spanish	Caribbean
Caribbean	English, French, Spanish	Caribbean
North American	English, French, Spanish	Canada, United States, Caribbean
Denmark	English, Danish	Denmark

System defaults

The following table compares the system defaults for the North American and Global market profiles. In addition, the following functionality applies:

- Market profiles for Denmark, Holland and Sweden are the same as the Global market profile except for the default to local languages and local tones and cadences.
- Market profile for Caribbean is the same as the North American profile except for its support for the M7000 phone.
- Market profile for CALA is the same as the Caribbean profile except NI ISDN replaced by ETSI ISDN (u-law).

Functionality	Attribute	North American	Global profile	United Kingdom
Direct Dial Access code		0	0	0
DTMF parameters	Tone duration	120 msec	120 msec	120 msec
	Pause time	1.5	1.5	3.5
	Interdigit time	80 msec	80 msec	100 msec
Conference tone		disabled	disabled	enabled
Call Back Kill time		180 sec	180 sec	360 sec
PCM Companding Law		mu-law	a-law EBI	a-law EBI
Race Integration		disabled	disabled	disabled
OLI digits		fixed 10 digits	fixed 10 digits	variable length up to 8
Dial Tone Detection		enabled	enabled	enabled
Hunt Groups	Show in second	disabled	disabled	disabled
	Default delay	4 ring cycles	4 ring cycles	4 ring cycles
	Queue timeout	60 sec	60 sec	60 sec
	If busy	busy tone	busy tone	busy tone
	Mode	broadcast	broadcast	sequential
Target line if busy setting		prime	prime	busy tone
M7000 set		disabled	enabled	enabled
Fax switch		enabled	enabled	enabled
Service Schedule time	Night	start 23:00 end 07:00	start 23:00 end 07:00	start 23:00 end 07:00
	Evening	start 17:00 end 23:00	start 17:00 end 23:00	start 17:00 end 23:00
	Lunch	start 12:00 end 13:00	start 12:00 end 13:00	start 12:00 end 13:00
	Service 4	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
	Service 5	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00
	Service 6	start 00:00 end 00:00	start 00:00 end 00:00	start 00:00 end 00:00

Functionality	Attribute	North American	Global profile	United Kingdom
Call Forward Delay	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	2 ring cycles
	Options	• 2 ring cycles • 3 ring cycles • 4 ring cycles • ring cycles • 10 ring cycles	• 2 ring cycles • 3 ring cycles • 4 ring cycles • ring cycles • 10 ring cycles	• 2 ring cycles • 3 ring cycles • 4 ring cycles • ring cycles • 10 ring cycles
DRT Delay	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	4 ring cycles
	Options	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • ring cycles • 10 ring cycles	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • ring cycles • 10 ring cycles	• 1 ring cycles • 2 ring cycles • 3 ring cycles • 4 ring cycles • ring cycles
Handsfree		none	none	none
Pickup Group		none	none	none
Remind Delay		60 secs	60 secs	60 secs
Allow SLR		disabled	disabled	disabled
Transfer Callback	Show in second	disabled	disabled	disabled
	Default	4 ring cycles	4 ring cycles	4 ring cycles
	Options	• 3 ring cycles • 4 ring cycles • 5 ring cycles • ring cycles • 12 ring cycles	• 3 ring cycles • 4 ring cycles • 5 ring cycles • ring cycles • 12 ring cycles	• 3 ring cycles • 4 ring cycles • 5 ring cycles • ring cycles • 12 ring cycles
Dialling Plan		market dependent (defined in application but controlled by market profile ID)	market dependent (defined in application but controlled by market profile ID)	market dependent (defined in application but controlled by market profile ID)
ONN Blocking	VSC for analog tone	n/a	n/a	141
	VSC for analog pulse	n/a	n/a	141
	VSC for BRI	n/a	n/a	141
	VSC for PRI	n/a	n/a	141
	State for BRI/PRI	n/a	n/a	send feature code
Default CO lines		2	2	4
UTAM		enabled	disabled	disabled
	Portable credits	0	defined in the application (max)	n/a

Functionality	Attribute	North American	Global profile	United Kingdom
Release reason	Release text	none	none	detail
	Release code	disabled	disabled	disabled
	Display duration	3 sec	3 sec	3 sec
Overlap Receiving		disabled	enabled	disabled
Local Number length for ISDN overlap receiving		8	8	8
Tandem alerting		disabled	disabled	disabled
TON/NPI		national/E.164	national/E.164	unknown/unknown
National number length		10	10	0
national number prepend		n/a	n/a	0
Provide tone on PRI		enabled	n/a	disabled

Glossary

A

AbsorbLength

A setting that determines how many of the digits in a destination code will not be dialed by the system. AbsorbLength is assigned under Destination codes in Services.

access code

Different sequences of characters used to gain access to the features: Line pools, Call park, external lines, Direct-Dial telephone and Auto DN.

address

A unique identifier assigned to networks and stations that allows each device to receive and reply to messages.

Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address that is recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. The physical machine address is also known as a Media Access Control or MAC address. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

alarm code

A number that is displayed, informing you that a fault has been detected in the system.

Analog Terminal Adapter

A device that permits the connection of analog telecommunication devices such as fax machines, answering machines, and single line telephones to the Enterprise Edge system.

ANSI

American National Standards Institute.

Answer button

A telephone button with an indicator that is used to monitor another telephone. The answer button indicates incoming calls destined for the other telephone. Someone working at a telephone with answer buttons (an attendant, for example) can receive all ringing and visual indication of incoming calls for other telephones, and answer those calls when necessary.

One telephone can have up to four Answer buttons. An Answer button is automatically assigned to a telephone when that telephone is assigned an Answer DN.

Answer DN

The internal or directory number (DN) of a telephone that is monitored by an Answer button. You can assign up to four Answer DNs to a telephone under Line Access in Terminals and Sets programming.

Application Program Interface (API)

An API is the specific method prescribed by an operating system or by another application program when a programmer writes an application program. The API is used to make requests of the operating system or another application.

Unlike the graphical user interface or command interface, which are direct user interfaces, the API is an interface to an operating system or a program.

Application

A computer program that performs a wide range of tasks as specified by the user. Examples of application programs include word processing packages, spreadsheet packages and accounting packages.

ARP

See Address Resolution Protocol.

asynchronous

A method of transmission where the time intervals between characters are not required to be equal and signals are sourced from independent clocks with different frequencies and phase relationships. Start and stop bits may be added to coordinate character transfer.

Autobumping

A feature that determines what the system does with new Call Log items when your Call Log is full. When Autobumping is on, a new log entry causes the oldest entry to be deleted. If Autobumping is off, your system does not log calls when your log is full.

autodial button

A memory button that, if programmed, provides one-touch dialing of external or internal numbers.

autolog options

A feature that allows you to select the type of calls that are stored in your Call Log. You can choose to log calls that were not answered by anyone within the system, to log calls that were unanswered at this telephone but answered elsewhere in the system, to log all calls answered and not answered at this telephone, or to not have calls automatically logged.

Automatic Daylight Savings Time

A feature that switches the system to standard or daylight savings time at pre-programmed times. It is turned on or off under Daylight time in System programming.

Automatic Dial

A feature that allows you to dial without having to pick up the receiver or select a line. You must have a prime line to use Automatic Dial. Automatic Dial is assigned under Dialing options in Terminals and Sets programming.

Automatic Handsfree

A feature which automatically activates Handsfree operation when you make or answer a call. Automatic Handsfree is assigned under Handsfree in Terminals and Sets programming.

Automatic Hold

A feature that automatically places an active call on hold when you select another line. Automatic Hold (Full AutoHold) is assigned in Lines programming.

Automatic Privacy

See Privacy.

Automatic Telephone Relocation

A feature that lets a telephone retain its personal and system programming when it is plugged into a different modular jack. Automatic Telephone Relocation is enabled under Set relocation in System programming.

auxiliary ringer

A separate external telephone ringer or bell which can be programmed to ring when a line or a telephone rings. An auxiliary ringer may be programmed to ring only when the system is in a particular schedule. Programming of an auxiliary ringer is done in Services programming after the feature has been enabled under Capabilities in Terminals and Sets programming.

AWG

American wire gauge.

B

B channel (Bearer channel)

An ISDN standard transmission channel used for voice or data transmission.

Background Music

A feature that lets you hear music from the speaker of your telephone. It is available only if a music source has been attached to the system and the feature has been enabled under Feature settings in System programming.

Back up

To make a duplicate copy of data files so that you can store the originals in a safe place. Backing up your original files protects them from damage if a hardware failure occurs.

Base Station

A Companion component that is mounted on walls and ceilings to provide a radio link to an office or other area where Companion portable telephones are used. Each Base Station houses two radios that allow portables to send and receive calls through the Enterprise Edge Server.

Basic Rate Interace (BRI)

An ISDN interface which uses two B channels and a D channel (2B+D). ETSI BRI is the European Telecommunications Standards Institute specification for BRI ISDN service

Baud rate

A unit of measurement of data transmission speed. It is approximately equivalent to Bits Per Second (BPS). Typical baud rates are 300, 1200, 2400, 4800, and 9600.

Bearer channel

See B channel.

BERT

See bit error rate test.

BIOS (Basic Input Output System)

A program contained in Read Only Memory (ROM) that acts as the interface between software programs and the computer hardware.

Bit

An abbreviation for Binary Digit. A bit is the smallest unit of information recognized by the computer. A bit has one of two values (0 or 1) to indicate off or on.

bit error rate test

A test that checks the transmission of data across the voice and data channels between the system and any telephone.

BPS (bits per second)

The speed of data transmission between two computers.

Bus

A collection of communication lines that carry electronic signals either between elements on the system board or between the circuitry on the system board and any cards plugged into the system board.

busy lamp field (BLF)

A device with a liquid crystal display (LCD) panel of indicators that shows the status of up to 24 telephones in the system.

Byte

The amount of space required to store a single character. One byte equals eight bits.

C

Call Duration timer

A feature that lets you see how long you spent on your last call or how long you have been on your present call.

Call Forward

A feature that forwards all the calls arriving at your telephone to another telephone in your system. To have calls forwarded outside the system, use Line Redirection.

Call Forward No Answer

A feature that forwards all calls arriving at your telephone to another designated telephone in your system after a specific number of rings. Call Forward No Answer is assigned under Capabilities in Terminals and Sets programming.

Call Forward On Busy

A feature that forwards all calls at your telephone to another designated telephone if your telephone is busy. This feature is assigned under Capabilities in Terminals and Sets programming.

Call Forward Override

An automatic system feature that lets you call someone and ask them to stop forwarding their calls to you.

Call Information

Call Information allows you to display information about incoming calls. For external calls, you can display the caller's name, telephone number and the line name. For an internal call, you can display the name of the caller and their internal number. You can obtain information about ringing, answered, or held calls.

Call Log

Enter your Call Log to view a record of incoming calls. The log could contain the following information for each call: sequence number in the Call Log, name and number of caller, long distance indication, indication if the call was answered, time and date of the call, number of repeated calls from the same source, and name of the line that the call came in on. See Autobumping, Autolog options, and Call Log for further information.

Call Park

With this feature you can place a call on hold so that someone can retrieve it from any other telephone in the system by selecting an internal line and entering a retrieval code.

The retrieval code appears on the display of your telephone when you park the call. You can park up to twenty-five calls on the system at one time.

Call Park Callback

See Callback.

Call Park prefix

The first digit of the retrieval code of a parked call. This digit cannot conflict with the first digit of any existing DNs, Line Pool access codes, the Direct-dial digit, or the external line access code. The default Call Park prefix digit is “1”. It may be set to none, in which case Call Park is disabled. Call Park prefix is assigned under Access codes in System programming.

Call Pickup Directed

A feature that lets you answer a call ringing at any telephone by entering the internal number of that telephone before taking the call. Call Pickup Directed is enabled under Feature settings in System programming.

Call Pickup Group

See Pickup Group.

Call Queuing

If you have several calls waiting at your telephone, you can invoke the Call Queuing feature to answer them in order of priority. Priority is given to incoming calls, followed by callback and camped calls.

Callback

If you park, camp, or transfer a call to another telephone and it is not answered there, it will ring again at your telephone. How long the system will wait before Callback occurs is set under Feature settings in System programming.

Camp-on

A feature that lets you reroute a call to a telephone even if all the lines on that telephone are busy. To answer a camped call, use Call Queuing or select a line if the camped call appears on your telephone. Priority is given to queued calls over camped calls.

Camp timeout

The length of a delay before a camped call is returned to the telephone that camped the call. The length of delay is set under Feature settings in System programming.

Central answering position (CAP)

An M7324 telephone that has been designated as a CAP under CAP assignment in System programming. The CAP provides backup answering and can be used to monitor the telephones within a system.

Central answering position (CAP) module

A module connected to an M7324 telephone and provides 48 additional buttons that can be used as autodial buttons or feature buttons. A maximum of two CAP modules can be connected to a single M7324 telephone.

Channel Service Unit (CSU)

A device on the Digital Trunk Interface that is the termination point of the T1 lines from the T1 provider. The CSU collects statistics on the quality of the T1 signal. The CSU ensures network compliance with FCC rules and protects the network from harmful signals or voltages.

Challenge-Handshake Authentication Protocol (CHAP)

CHAP is a method of establishing security on PPP links where the peers must share a plain text identifier. The caller sends a challenge message to its receiving peer and the receiver responds with a value it calculates based on the identifier. The first peer then matches the response with its own calculation. If the values match, the link is established.

CHAP is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP).

Class of Service (COS)

The set of features and lines available to the user for a call. The Class of Service for a call is determined by the restriction filters and remote access packages assigned to the telephone in Lines programming. The Class of Service for a call can be changed by entering a six-digit Class of Service password. (Internal users cannot change their access to features with a COS password, only their restriction filters.) Class of Service and Class of Service passwords are assigned in Passwords programming. See Remote Access.

Class of Service password

A six digit code that lets you switch from your current Class of Service to one that lets you dial numbers prohibited by your current Class of Service.

client

A client is a computer system or process that requests a service of another computer system or process. A workstation requesting the contents of a file from a file server is a client of the file server.

cold start

A cold start occurs when all system programming is lost. This can happen after a major event such as an extended power failure.

Companion portable telephone

Hand-held wireless telephones that allow complete mobility within the reach of Companion Base Stations or an external antenna. Portables offer many but not all standard system features and share much of the same programming as “wired” desk telephones.

Companion Wireless

The name for the communication systems which use radio technology to transmit and receive signals between its components and the Enterprise Edge Server. Companion Wireless provides mobility in the workplace. Calls that used to ring just at your telephone set can also appear and ring at your portable.

Conference

A feature that allows you to establish a three-person call at your telephone.

Conventions

The way certain information is described. For example, using underlined text to represent second-line display prompt information.

COS

See Class of Service.

D

D channel (Data channel)

An ISDN standard transmission channel which is packet-switched, and is used for call setup, signalling and data transmission.

Data channel

See D channel.

Data link connection indentifier (DLCI)

The DLCI is used to identify a PVC in frame relay networks.

Defaults

The settings for all features when the system is first installed. Settings are changed from their defaults in programming.

Delayed Ring Transfer (DRT) to prime

After a specified number of rings, this feature transfers an unanswered call on an external line to the prime telephone associated with that line. This feature is activated under Feature settings in System programming.

destination code

A two- to seven-digit number that the system interprets and then translates into the digits that you want dialed out. Both the code and its associated dialed digits are assigned under Routing service in Services programming.

DHCP

See Dynamic Host Configuration Protocol.

dialing restriction

See Restriction filter.

dial-up connection

A dial-up connection is a temporary connection between computers that is established over an analog or digital phone line.

Differentiated Services (DiffServ)

DiffServ is an implementation methodology for QoS service for IP networks. DiffServ is a rule based methodology intended to improve network performance. Instead of applying faster, more advanced technology, networks are managed by appropriate network policies. With DiffServ there is a cost associated with higher quality services and a risk with lower quality services.

Digital Access Signaling System Number 2 (DASS2)

A UK proprietary standard for signalling on ISDN connections between customers' premises and the public network. DASS2 is used between the customer's equipment and ISDN local exchange and is suitable for multiple access.

Digital Private Network Signalling System (DPNSS)

DPNSS is a networking protocol that gives operators access to Enterprise Edge features over multiple combined networks in International systems only. Corporate offices, separated geographically, can be linked over DPNSS to other Enterprise Edge systems, bypassing the restrictions of the PSTNs to which they may be connected. This allows connected Enterprise Edge systems to function like a private network.

Direct-dial

A feature that lets you dial a designated telephone in your system with a single digit. As many as five direct dial sets can be established. Each telephone in the system is assigned to one direct-dial telephone. There is a single, system wide digit for calling the assigned direct-dial telephone of any telephone. Direct-dial telephones are established in System programming. Telephones are assigned to a direct-dial telephone under Capabilities in Terminals and Sets programming.

Direct-dial

A digit used system-wide to call the Direct-dial telephone. The digit is assigned under Access codes in System programming.

Direct-dial number

The digit used to call the direct-dial telephone.

directed pickup

See Call Pickup Directed.

Directory number (DN)

A unique number that is automatically assigned to each telephone or data terminal. The DN, also referred to as an internal number, is often used to identify a telephone when settings are assigned during programming.

Disconnect Supervision

A setting that enables the system to detect whether an external caller hangs up. Once an external caller hangs up, the system can disconnect its line. Disconnect Supervision is enabled under Trunk/Line data in Lines programming.

Disk drive

A mass storage device that seeks, reads and writes data on a disk.

Display

A one-line or two-line screen on an Enterprise Edge telephone that shows commands and options.

Display buttons

The three buttons that appear underneath an Enterprise Edge two-line LCD display.

Display options

The choices available to a user that appear on the Enterprise Edge two-line display. Options appearing on the display can be selected using the display or dialpad buttons.

DLCI

See Data link connection indentifier.

DN

See Directory number (DN).

DNS

See Domain Name Server (DNS).

DNS proxy

A Domain Name Service (DNS) proxy translates alphabetic domain names into computer-readable IP addresses. For example, the domain name www.nortelnetworks.com for the Nortel Networks web site can translate to the IP address 192.177.5.18. After a domain name is translated into an IP address, the workstations on your network can communicate with the web site. Depending on the configuration of your system, you can let your workstations know that Enterprise Edge is the DNS proxy.

domain name

The domain name is used to organize Internet names into manageable groups, such as nortelnetworks.com, where nortelnetworks is the domain name.

Domain Name Server (DNS)

The domain name system or domain name server is the system in the Internet that maps names of objects, most usually host names, into IP numbers or other resource record values. The namespace of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain.

Do Not Disturb

A feature that stops calls from ringing at your telephone. Only Priority Calls will ring at your telephone. A line button will flash when you receive a call, but the call will not ring.

Driver (Device)

A program that allows a hardware peripheral, such as a NIC, to communicate with the Enterprise Edge Server.

DTMF

See Dual tone multifrequency.

dual tone multifrequency

Two distinct telephone signaling tones used for dialing.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

dynamic IP address

A dynamic IP address changes. Dynamic IP addresses are assigned to computers by an IP address server as the computer needs it. Usually there is a particular range, or scope, of IP addresses that your network uses. With dynamic IP addressing, a computer can have a different IP address every time it connects to the network. Other devices must know the computer’s IP address so that they can communicate with it. The IP address server manages the assignment of IP addresses to the client workstations. See also static IP address.

E

Emergency 911 dialing

The capability to access a public emergency response system by dialing the digits 9-1-1. State and local requirements for support of Emergency 911 Dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations.

emergency telephone

A single-line telephone (also referred to as a 500/2500 telephone) that becomes active when there is no power to the Enterprise Edge Server.

Ethernet

A widely used Local Area Network (LAN) protocol that is the original Carrier Sense Multiple Access/Collision Detect (CSMA/CD) LAN that lets PCs and/or Enterprise Edge Servers listen for pauses before they communicate. Ethernet LANs use coaxial cable or twisted pair wiring for connecting computers.

evening schedule

See Schedules and Services.

event message

Event messages are stored in the system log and displayed during a Maintenance session. They record a variety of events and activities in the system.

exceptions

See Overrides.

Extended Data-Out (EDO)

A form of Dynamic Random Access Memory (RAM) in which storing data to and reading data from the memory is performed at a faster rate.

external call

A call to a destination outside the system.

external code

The number you dial to get an external line. By default it is 9, but this can be changed under Access codes in System programming. You do not always need an external code. It is primarily to support the M7100 telephone and single line telephones using an Analog Terminal Adapter.

external line

A line on your telephone used for making calls to destinations outside the system.

external music source

See Music source.

external paging

A feature you can use to make voice announcements over an externally-mounted loudspeaker connected to the Enterprise Edge Server. The external speaker is not an Enterprise Edge component and must be supplied by the customer.

F

FAX

FAX works with Enterprise Edge Voice Messaging, offering a caller the capability of sending a fax document to a mailbox as easily as sending a voice message.

Feature Code

A unique code used to access Enterprise Edge features and options.

File

A collection of related information stored on a disk under a given name for later reference and used by an operating system or application program. Each application program that you use saves the data you create in files. Files are identified by a file name and optional extension.

File name

A name that identifies a file and consists of one to eight characters.

filtering

Filtering is the process of examining a data packet on the network to determine the destination of the data and whether the packet should be passed along on the local LAN, copied to another LAN, or dropped.

Forward

See Call Forward.

frame

A frame is a unit of data transmission in a local area network.

frame relay

A frame relay is a high-speed, packet switching WAN protocol designed to provide efficient, high-speed frame or packet transmission with minimum delay. Frame relay uses minimal error detection and relies on higher level protocols for error control.

FTP

The file transfer protocol (FTP) allows a user on one host to access and transfer files to and from another host over a network. On the Internet, FTP refers to a tool for accessing linked files.

Full Autohold (on idle line)

When this feature is on, if you select an available line, and then do something that selects another line, the first line is put on hold. Full Autohold is enabled under Trunk/Line data in Lines programming.

Full Handsfree

See Handsfree.

Fully Qualified Domain Name (FQDN)

The combination of host name and domain name. For example mycomputer.nortelnetworks.com is Fully Qualified Domain Name.

G

gateway

A system that links two different types of networks and enables them to communicate with each other. Enterprise Edge is the gateway that links your company's network to the Intranet or Internet. Depending on your configuration, you can let your workstations know that Enterprise Edge is your Internet gateway.

Ground Start trunk

Ground start trunks offer the same features as loop start trunks, but are used when the local service provider does not support disconnect supervision for the digital loop start trunks. By configuring lines as ground start, the system will be able to recognize when a call is released at the far end. Ground start trunks are provided only by a Digital Trunk Interface (DTI).

Group Listening

A feature that allows you to have others in your office hear a caller through your telephone speaker. The caller hears you only when you speak into the receiver and cannot hear other people in the office.

You can cancel Group Listen for the current call. Group Listen is cancelled automatically when you hang up the Group Listen call.

H

H.323

H.323 is the standard for using IP to send voice and video within intranets and on the public Internet.

Handsfree

A feature you can use to make calls without using the telephone receiver. Full Handsfree is activated under Capabilities in Terminals and Sets programming. When it is activated, a Handsfree/Mute button is automatically assigned to the telephone.

Handsfree (HF) Answerback

When activated, this feature automatically turns on the microphone at a telephone receiving a Voice Call so that the person receiving the call can respond without lifting the receiver. It is activated under Capabilities in Terminals and Sets programming.

Handsfree/Mute button

See Handsfree.

Hard disk drive

A data storage device that uses non-removable, rigid magnetic platters. Hard disk drives work faster and store more data than disk drives do for diskettes.

Hardware

The physical components of the Enterprise Edge system.

HDLC

See High-level Data Link Control.

Headset

A head-mounted or ear-mounted telephone receiver that is used instead of the hand-held receiver. Headsets are not Enterprise Edge system components and must be supplied by the customer.

Held (Line) Reminder

A telephone rings and displays the message **On hold: LINENAM** when an external call has been placed on hold for a certain period of time. The Held Line Reminder feature and Remind delay are set under Ftr settings in System programming.

HF Answerback

See Handsfree Answerback.

High-level Data Link Control (HDLC)

HDLC is a group of protocols or rules for transmitting data between network points or nodes. Data is organized into a unit, called a frame, and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in Layer 2 of the industry communication reference model, Open Systems Interconnection (OSI).

Hold button

This button is used to suspend calls so that the person using the telephone can perform another task without disconnecting the caller.

Hook Switch Flash

See Link time.

Host Name

In networking, the name of a computer that primarily provides services, such as database access, to other computers or Enterprise Edge Servers in the domain. The host name is associated with a unique IP address. Since the Enterprise Edge Server has a unique IP address, it qualifies as a host.

Host system signaling

Also referred to as end-to-end signaling. Telephones can access a remote system or dial a number on an alternate carrier by means of host feature activation, such as Link, Pause and Run/Stop.

Hotline

This feature automatically calls a pre-assigned number when the telephone's receiver is lifted or the Handsfree/Mute button is pressed. A Hotline number can be an internal or external number. Hotline is assigned under Capabilities in Terminals and Sets programming.

HTTP

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the world wide web.

HTTP proxy

See Web proxy.

Hz (hertz)

A unit of measure for indicating frequency in cycles per second.

I

I/C

An abbreviation of intercom.

ICMP

ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, however the messages are processed by the TCP/IP software and are not directly apparent to the application user.

IETF

See Internet Engineering Task Force.

In-Band

In-band is a method of device access which utilizes a network interface component within the device.

Initialization

The steps required to prepare hardware or software for operation.

Install

To set up for operation. For example, hardware is installed by attaching it to the appropriate connectors or sockets either inside or outside the Enterprise Edge Server.

Integrated Services Digital Network (ISDN)

A digital telephone service that allows for a combination voice and data connection over a single, high-speed connection. ISDN service can operate over the same copper twisted-pair telephone line as analog telephone service.

intercom button

A button that provides access to internal lines used for calls within a Enterprise Edge system and access to external lines through a line pool or external code. A telephone may be assigned zero to eight Intercom buttons. This is done under Line access in Terminals and Sets programming.

intercom keys

See Intercom button.

Interface

An information interchange path that allows communication between computer parts.

internal line

A line on your telephone dedicated to making calls to destinations inside your system. An internal line may still connect you with an external caller if you use it to access a line pool or to pick up a call using the call handling features such as Call Park or Call Pickup Directed.

internal number

A number (also referred to as a Directory Number or DN) that identifies a telephone or device.

internal user

Someone using an Enterprise Edge telephone within the system.

Internet

A global TCP/IP network linking millions of computers for communications purposes.

Internet Engineering Task Force (IETF)

The IETF is the committee that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society's Internet Architecture Board (IAB).

Internet-standard Network Management Framework

Device configuration and monitoring via SNMP.

IP

The Internet Protocol (IP) is the protocol that supports data being sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. When you send or receive data, the message gets divided into units called packets. Each of these packets contains both the sender's Internet address and the receiver's address.

IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

IP address

The Internet Protocol address is a unique identifier that allows communication over the Internet to be directed to the appropriate destination. Every computer on the Internet must have a unique IP address. IP addresses are allocated by an Internet service provider (ISP) in the following format: nnn.nnn.nnn.nnn, where nnn is a numeric value from 0 to 255. IP addressing might be referred to as being static IP address) or dynamic IP address.

IPX

IPX (Internetwork Packet Exchange) is a networking protocol from Novell that interconnects networks that use Novells NetWare clients and servers. IPX is a datagram or packet protocol. IPX works at the network layer of communication protocols and is connectionless (that is, it doesn't require that a connection be maintained during an exchange of packets as, for example, a regular voice phone call does).

IRQ (Interrupt Request)

A signal sent by a hardware device to the microprocessor requesting its immediate attention. For example, each communications port has an interrupt request line for notifying the microprocessor when data has been received or transmitted.

IRQ Conflict

Two hardware devices are vying for same IRQ. On installation of a device where an IRQ conflict occurs, the user may have to manually configure the IRQ settings to resolve the conflict.

ISDN

See Integrated Services Digital Network.

ISDN DN

A directory number (DN) used by ISDN terminal equipment connected to the system. The Enterprise Edge system uses a maximum of thirty ISDN DNs.

K

Kbyte

The abbreviation for kilobyte. A kilobyte is equal to 1024 bytes.

L

LAN

A LAN is a network of interconnected workstations sharing the resources of a single processor or server within a relatively small geographic area.

Last Number Redial

A feature that allows you to redial the last external number you dialed.

Least cost routing

See Routing service.

line

The complete path of a voice or data connection between one telephone (or other device) and another.

Line number

A number that identifies an external line. The total number of lines depends on the number and type of trunk media bay modules installed.

Line Pool

A group of lines used for making external calls. Line pools provide an efficient way of giving a telephone access to external lines without taking up many line buttons. A line is assigned to be part of a line pool under Trunk/Line data in Lines programming.

Line Redirection

A feature that allows you to redirect all calls on an incoming line to a destination outside the system. Once a line is redirected it cannot be answered within the system. The system may be set up to give a brief ring when a call comes in on a redirected line, under Capabilities in Terminals and Sets programming.

This feature differs from Call Forward in two ways. It redirects only external calls (not internal calls) and it redirects calls to destinations outside the system. Call forward redirects calls only to destinations inside the system. See Call Forward.

Lines

A programming section that lets you assign settings to each trunk and external line.

Link

If your Enterprise Edge system is connected to a Private Branch Exchange (PBX), you can use a Link signal to access special features. The Link signal can also be included as part of a longer stored sequence on an External Autodial button or in a Speed Dial code. The Link symbol uses two of the 24 spaces in a dialing sequence.

Local Area Network (LAN)

A group of computers or Enterprise Edge Servers physically connected in a manner that lets them communicate and interact with each other.

Long Tones

A feature that lets you control the length of a tone so that you can signal devices such as fax or answering machines which require tones longer than the standard 120 milliseconds.

Lunch schedule

See Schedules and Services.

M

M7100 telephone

The Enterprise Edge model M7100 telephone that has a single-line display and one programmable button without an indicator.

M7208 telephone

The Enterprise Edge model M7208 telephone that has a single-line display and eight programmable buttons with indicators.

M7310 telephone

The Enterprise Edge model M7310 telephone that has a two-line display with three display buttons, 10 programmable buttons with indicators and 12 dual programmable buttons without indicators.

M7324 telephone

The Enterprise Edge model M7324 telephone that has a two-line display with three display buttons and 24 programmable buttons with indicators.

MAC

The Media Access Control (MAC) is a physical address that is the portion of the data-link layer in 802.x networks that controls addressing information of the packet and enables data to be sent and received across a local area network.

Maintenance

A type of programming that is used to diagnose and repair problems in the Enterprise Edge system. Maintenance requires no programmable settings.

Mailbox

A storage place for voice messages on Enterprise Edge Voice Messaging.

Meridian 1 ISDN Primary Rate Interface (MCDN)

A protocol used between members of the Nortel Networks Meridian family of Private Telecommuncation Network Exchanges. The signalling information is carried via time slot 16 of a 2.048 Mbit/s digital transmission system.

message

A feature that allows you to send a message to another system user. The Message feature also lets you know if you have any messages waiting and maintains a Message Waiting List to keep a record of your internal messages and your (external) voice mail messages.

MHz

The abbreviation for megahertz. This is a unit of measure indicating frequency in millions of cycles per second.

Microprocessor

A chip that is the center of all activity inside the Enterprise Edge Server. The microprocessor controls all logical and arithmetic operations for the computer and is responsible for executing program commands. It is also referred to as the Central Processing Unit (CPU).

Modem

A communications device that allows data to be exchanged between computers over telephone lines. The exchange is done by electronic processes called modulation and demodulation. The modem changes (modulates) the data into tones to send to another modem and also converts (demodulates) tones when receiving from another modem.

Move Line buttons

A feature that allows you to move external lines to different buttons on your telephone.

Multilink PPP

Multilink PPP is an extension to the PPP protocol that enables you to group a set of links into abundle for more bandwidth. The links in the bundle can operate at different speeds. Typical links can be ISDN B channels, dial-up connections, and leased-lines.

Music source

A radio or other source of music can be connected to the system to provide music for the Music on Hold and Background Music features. A music source is not part of the Enterprise Edge system and must be supplied by the customer.

N

Names

Names can be assigned to System Speed Dial numbers, external lines, telephones, mailboxes, ACD Queues and service schedules. This is done in programming. You can use up to sixteen characters to name a System Speed Dial number, 13 characters for mailbox and ACD Queue names, and seven characters to name a telephone, line, or schedule.If a Name has not been assigned, the line number or DN will appear on the display instead of a name.

name server

A name server provides the means of translating readable host computer names into actual IP addresses so you do not have to remember long numbers in order to access other computers and destinations on the Internet. For example, DNS servers and WINS servers are name servers.

NetBIOS

The Network Basic Input/Output System (NetBIOS) is an interface and upper-level protocol developed by IBM for use with a proprietary adapter for its PC network product. NetBIOS provides a standard interface to the lower networking layers. The protocol provides higher-level programs with access to the network. Windows NT systems use NetBIOS.

Network

Two or more computers linked together electronically to share programs and exchange data. Joining computers over a network requires adding specialized hardware and software to each computer.

network device

A network device is a hardware entity characterized by its use as a communications component within a networking infrastructure.

Network DN

A number supplied by the ISDN network service provider for ISDN terminal equipment.

Network Interface Card (NIC)

An adapter card containing the hardware necessary to connect an Enterprise Edge Server to a local area network.

NIC

A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network.

Personal computers and workstations on local area networks (LANs) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or Token Ring. Network interface cards provide a dedicated, full-time connection to a network.

Night schedule

See Schedules, and Services.

O

On hold

A setting, programmed under Feature settings in System programming, that controls whether external callers hear music, periodic tones, or silence when they are placed on hold.

Open Shortest Path First (OSPF)

A routing protocol used within larger autonomous and complex networks in preference to the Routing Information Protocol (RIP) which suits a small network. Like RIP, OSPF is designated by the Internet Engineering Task Force as one of several Interior Gateway Protocols.

Operating system

The disk-based software that manages the operation of the Enterprise Edge Server. An operating system controls the flow of information between the computer hardware. Windows® NT is the operating system that manages the Enterprise Edge Server.

option

An Enterprise Edge Server choice that is given to a user through display prompts.

OPX

Off premise extension.

OSPF

See Open Shortest Path First (OSPF).

Out-of-Band

Out-of-band is a method of device access which circumvents the network interface components within the device.

overflow

A setting in Routing Service that allows users to decide what path an outgoing call will take if all the lines used in a particular route are in use when the call is made.

Overrides

One component of a restriction filter. Overrides are numbers you can dial even if they are forbidden by a more general restriction. See Restrictions.

P

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into pieces of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When the packets have all arrived, they are reassembled into the original file.

A packet-switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit-switching, is used for networks allocated for voice connections. In circuit-switching, lines in the network are shared among many users as with packet-switching, but each connection requires the dedication of a particular path for the duration of the connection.

Packet and *datagram* are similar in meaning. A protocol similar to TCP, the User Datagram Protocol (UDP) uses the term datagram.

Page

A feature you can use to make announcements over the Enterprise Edge system. You can make page announcements over the telephone speakers and/or external speakers.

Page Time out

A setting that controls how long a Page Announcement can last. It can be assigned under Feature settings in System programming.

Page zone

An area in the office that receives internal page announcements independently of the rest of the office.

Each page zone is identified by a number. Telephones are assigned to page zones under Capabilities in Terminals and Sets programming.

PAP

The Password Authentication Protocol (PAP) is a procedure used by PPP servers to validate a connection request. PAP works as follows:

1. After the link is established, the requestor sends a password and an id to the server.

2. The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance.

Passwords are sent without security and the originator can make repeated attempts to gain access. For these reasons, a server that supports CHAP will offer to use that protocol before using PAP.

Parallel port

A port that transfers data through multiple wires so that eight bits are transmitted simultaneously. Parallel ports usually use a 25-pin interface that transmits and receives data one byte at a time using a separate data line for each bit.

Park prefix

See Call park prefix.

Park timeout

The time before an unanswered parked call is routed back to the telephone that parked it. Park timeout is under Feature settings in System programming.

Password

A four-digit to eight-digit number that is entered using the dialpad. A password is used to open mailboxes or perform configuration tasks.

Pause

A feature that enters a 1.5 second delay in a dialing sequence on an external line. This is often required for signaling remote devices, such as answering machines, or when reaching through to PBX features or host systems. The Pause symbol uses one of the 24 spaces in a dialing sequence.

PBX

See Private branch exchange.

Peripheral Component Interconnect (PCI) Slot

Socket on the Enterprise Edge Server main board that connect to the Enterprise Edge cards.

Permanent virtual circuit (PVC)

The PVC is an end-to-end virtual connection in frame relay networks.

Personal Speed Dial

Two-digit codes (71-94) can be programmed to dial external telephone numbers. Personal Speed Dial numbers are programmed for each telephone, and can be used only at the telephone on which they are programmed.

Pickup Group

A telephone can be placed into one of nine call pickup groups. A call ringing at a telephone within a pickup group can be picked up at any other telephone within the same pickup group. A telephone is assigned to a pickup group under Capabilities in Terminals and Sets programming.

Pin-1

The first pin in a multiple-pin connector or chip designated as such to help you properly orient the component when attaching or installing it.

Point-to-point protocol (PPP)

PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connects to a server by a phone line. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

Pool

See Line pool.

Port

A connector on the Enterprise Edge Server that allows data exchange with other devices, such as a printer or mouse.

portable telephone

See Companion portable telephone

PPP

See Point-to-point protocol.

Pre-dial

A feature that allows you to enter a number and check it on your telephone display before it is actually dialed. If the number is incorrect, you can edit it. The number is dialed only when you pick up the receiver or select a line.

Primary Rate Interface (PRI)

An ISDN interface that uses twenty three B channels and a D channel (23B+D).

Prime line

The line on your telephone that is automatically selected when you lift the receiver, press the Handsfree/Mute button or use an external dialing feature. A Prime Line is assigned to a telephone under Line access in Terminals and Sets programming.

Prime Set (prime telephone)

A telephone that provides backup answering for incoming calls on external lines. The prime telephone for a line will ring for any unanswered calls on that line. A prime telephone is assigned to a line under Trunk/Line data in Lines programming.

Priority Call

If you get a busy signal when you call someone in your office, you can interrupt them for an urgent call. This feature is enabled for a telephone under Capabilities in Terminals and Sets programming.

Privacy

This feature determines whether a system user may select a line in use at another telephone and join an established call. Privacy is enabled under Trunk/Line data in Lines programming, but can be turned on and off by users during individual calls.

Private branch exchange (PBX)

A PBX is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

The PBX is owned and operated by the enterprise rather than the telephone company.

Private line

See Private to.

Private network

A telephone network consisting of owned or leased telephone lines used to connect different offices of an organization independently of the public network.

Private to

Lets you select the telephone that will use the line exclusively. The line cannot appear on any other telephone, except the prime telephone for that line. Private lines cannot be placed into line pools. Private lines are assigned under Trunk/Line data in Lines programming.

programming

Setting the way the Enterprise Edge system will work. Programming includes system-wide settings and individual telephone and line settings.

Protocol

A set of rules and procedures for exchanging data between computers or Enterprise Edge Servers on a network or through the Internet.

Power cable

A cable that connects the Enterprise Edge Server to apower source.

Proxy

A proxy is a server that acts on behalf of another.

Power cable

A cable that connects the Enterprise Edge Server to apower source.

public line

An external line that can be assigned to any telephone and to many telephones. A line is assigned as Public under Trunk/Line data in Lines programming.

public network

The regular telephone network that connects most homes and businesses.

pulse/tone dialing

An external line setting for pulse or tone dialing. Pulse is the traditional method of dialing used by rotary-dial or push-button single-line telephones. Tone dialing allows telephones to communicate with other devices such as answering machines. Tone dialing is required to access the features that PBX systems may offer or to use another system remotely.

PVC

See Permanent virtual circuit.

Q

Quality of Service (QoS)

On the Internet and in other networks, QoS refers to guaranteed throughput level. QoS allows to measure, improve and, to some level, guarantee the transmission rates, error rates, and other data transmission characteristics. QoS is critical for the continuous and real-time transmission of video and multimedia information which use high bandwidth.

QoS

See Quality of Service (QoS).

Q reference point signalling (QSIG)

QSIG is an ETSI standard signalling for multi-vendor peer-to-peer communications between PBXs and/or central offices.

R

RAM (Random Access Memory)

Computer memory that stores data temporarily. RAM stores the data used by the microprocessor as it executes instructions. The contents of RAM are erased each time the Enterprise Edge Server is turned off or restarted.

receiver

The handset of a telephone.

Regression Code

Restores the previous system security number so that previously applied UTAM Activation Codes and Portable Credit Codes can be reentered to restore full system operation. Also required in cases of system recovery. This code cannot be reused.

Relaying

Relaying is the process of moving data along a path determined by a routing process. The data is relayed between a source and a destination.

Remind delay

A feature that causes a telephone to beep and display the message `On hold: LINENAM` when a call has been on hold for a programmable period of time. This period is the Remind delay.

Remote access

The ability to dial into an Enterprise Edge system from outside the system and make use of selected features. The lines, features, and dialing capabilities available to a remote user are determined by the Class of Service.

remote access dial restriction

See Remote restriction.

Remote access service (RAS)

The RAS is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporation's network. Home users get access to the Internet through remote access to an Internet service provider (ISP).

A remote access server is the computer and associated software that is set up to handle users seeking access to network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

Remote capability

A subset of Enterprise Edge features that are available to users connected through remote access.

Remote device

A remote device is any network device that is accessible only by means of communication over a digital or analog (dial-up) network.

Remote monitoring

A feature that lets an off-site technician with a PC call in and troubleshoot your system through the built-in modem.

Remote paging

This feature allows remote users to use the system paging feature. Access to this feature is governed by the Class of Service for the call. See Remote Access and Class of Service.

Remote restriction

A restriction filter applied to a line in order to control which digits can be dialed during an incoming remote access call. It is the equivalent of a set filter for a remote user.

remote user

Someone who calls into an Enterprise Edge system from a telephone outside that system and uses system features or lines. See Remote Access.

Restriction filter

Through a combination of restrictions and overrides, restriction filters prevent certain telephone numbers or feature codes from being dialed. Restriction filters can be applied to lines, sets, specific lines on a set, and to Class of Service passwords.

Restriction service

A Services section that allows you to assign alternate dialing filters to lines, telephones, lines on a particular telephone, and alternate remote filters to lines at specified times of the day and on specified days.

restrictions

One component of a Dialing filter. Restrictions are numbers you cannot dial when that dialing filter is in effect. See Exceptions.

Ring Again

A feature that can be used when you cannot get through to someone on your system because their telephone is busy or there is no answer. Ring Again instructs the system to inform you when they hang up or next use their telephone.

ring group

A setting under Services that lets you assign a number of different telephones to ring during one of the schedules. Up to 20 ring groups can be programmed by an installer or a system coordinator plus.

ring type

A feature that allows you to select one of four distinctive rings for your telephone.

ring volume

A feature that allows you to set the volume at which your telephone rings.

ringing service

A Services section that allows you to make additional telephones ring at specified times of the day and on specified days.

RIP

See Routing Information Protocol.

Rls button

Ends a call in the same way that hanging up the receiver does.

ROM (Read Only Memory)

Memory that stores data permanently. ROM contains instructions that the Enterprise Edge Server needs to operate. The instructions stored in ROM cannot be changed and are used by the Enterprise Edge Server each time it is turned on or restarted.

Router

A router is a device that forwards traffic between networks, based on network layer information and routing tables. A router decides which path network traffic follows using routing protocols to gain information about the network and algorithms to choose the best route based on a routing matrix.

Routing

The path a message takes from its point of origin to its destination on a network or the Internet.

Routing Information Protocol (RIP)

RIP enables routers in the same autonomous system to exchange routing information by means of periodic updates. RIP is a widely-used protocol for managing routing information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs.

Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts is has on record) to its closest neighbor host every 30 seconds. The neighbor host passes the information to its next neighbor and so on until all hosts within the network have the same routing path information, a state known as network convergence. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network.

The major alternative to RIP is the Open Shortest Path First Protocol (OSPF).

Routing service

A programming section that allows outgoing calls to be directed automatically based on the numbers a caller dials. For Enterprise Edge Servers linked in a network, routing can create a transparent or coordinated dialing plan. It can also be used to direct calls to the least expensive lines according to a Services schedule (sometimes called least cost routing).

Run/Stop

A feature that creates a break point in a programmed external dialing sequence. When you press a programmed key, the system dials the number up to the run/stop. When you press it again, the system dials the digits following the run/stop.

S

SAPS

See Station Auxiliary Power Supply.

Saved Number Redial

A feature that allows you to save the number of the external call you are on (providing you dialed the call) so that you can call it again later.

Schedules

Any of six different sets of services that can be applied to your system. See Services.

Selective line redirection

See Line Redirection.

Serial port

A port that sends and receives data one bit at a time. This port can be used to connect the Enterprise Edge Server to a printer, external modem or mouse. Serial port connector has nine pins and are designated by software with the letters COM and a single digit, such as COM1.

Service modes

See Services.

Service profile identifer (SPID)

A number that identifies the services ordered with your ISDN BRI line. Each ISDN BRI line has two phone numbers. Each of these phone numbers has a SPID. (See also SPID on page 430.)

Services

A programming section that lets you assign which telephones ring, which restrictions apply, and which call routing is used during any of six different schedules. There are three services: Ringing service, Restriction service and Routing service, all found in Services programming.

set

A telephone.

Set Copy

A programming section that allows you to copy programmable settings from one telephone to another of the same type. Set Copy provides two options: duplicating System Data and User Data, or duplicating System Data only. Set Copy does not provide the same copy capability as COPY, which is more selective of the settings that can be duplicated.

Set filter

See Restriction filter.

Set lock (telephone lock)

This feature allows you to limit the number of features that may be used at a telephone. Full set lock allows very few changes or features, Partial set lock allows some changes and features, and No set lock allows any change to be made and any feature to be used. Set lock is assigned under Capabilities in Terminals and Sets programming.

Set relocation

See Automatic Telephone Relocation.

SIMM

Single In-line Memory Module. The Enterprise Edge Server is equipped with one SIMM that provides 64 MB of SDRAM. The memory can be increased with the addition of more SIMMs.

Simple Network Management Protocol (SNMP)

SNMP is the protocol governing network management and the monitoring of network devices and their functions.

Software keys

A programming section used to enable the optional Remote monitoring feature. One setting provides a System ID, which an installer or system coordinator plus then uses to request three password keys from the Nortel Networks Customer Response Center. Once these three passwords have been entered, the system will permit Remote monitoring.

SPID

Acronym for Service Profile Identifier, a number that identifies a specific ISDN line. When you obtain ISDN service, your telephone company assigns a SPID to your line. Part of the initialization procedure is to configure your ISDN terminal adapter to use this SPID.

Most telephone companies in North America use the Generic SPID Format, which is a 14-digit number. The first 10 digits identify the telephone number, called the Directory Number (DN). The remaining four digits identify a particular ISDN device, in the case where multiple devices share the same Directory Number. (See also Service profile identifer (SPID) on page 428.)

Startup programming

When an Enterprise Edge system is first installed and powered up, Startup programming must be performed before any programming can be done. Startup initializes the system programming to defaults.

static IP address

A static or fixed IP address never changes. It is assigned to a computer permanently. The computer has the same IP address every time it connects to the network and is known to other devices on the network by that IP address. Compare with dynamic IP address.

Station

An individual telephone.

Station Auxiliary Power Supply (SAPS)

A device which provides power to a telephone that is connected more than 300 m (975 ft.) and less than 1200 m (3900 ft.) from the server, or to a CAP module.

Station Media Bay Module

A computer module which provides access to telephone lines. The 16-port Digital Station Media Bay Module (EE-DSM 16) allows the connection of 16 digital telephone sets to the system. The 32-port Digital Station Media Bay Module (EE-DSM 32) allows the connection of 32 digital telephone sets to the system. The Analog Station Media Bay Module (EE-ASM 8) allows the connection of analog station sets to the system.

Station set test

A series of diagnostic tests for these components of a telephone: display, buttons, handset, speaker, and power.

subnet mask

A value used to route packets on TCP/IP networks. When the IP layer has to deliver a packet through an interface, it uses the destination address contained in the packet, together with the subnet mask of the interface to select an interface, and the next hop in that subnet

synchronous

A synchronous signal is sourced from the same timing reference. A synchronous signal causes the interval between successive bits, characters, or events to remain constant or locked in to a specific clock frequency.

system data

An option in the Set Copy function. System Data refers to the programmable system settings that apply to all telephones and lines.

System programming

A programming section that lets you assign and maintain certain settings on the Enterprise Edge system.

System speed dial code

A two-digit code (01 to 70) that can be programmed to dial a telephone number up to 24 digits long. System speed dial codes are programmed for the entire system under the System Speed programming heading.

System Startup

See Startup programming.

T

T1

Digital carrier system or line that carries data at 1.544 Mbps.

TAPI

See Telephony Application Program Interface.

Target lines

Lines used to answer incoming calls only. A target line routes a call according to digits it receives from an incoming trunk. They are referred to by line numbers in the same way as physical lines.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

TE

See Terminal equipment.

TEI

See Terminal Endpoint Identifier.

Telco features

A programming section that lets you specify the external telephone numbers that are dialed by the Message feature to retrieve voice messages, or to set up CLASS (CMS) services for lines and telephone. Telco features are accessed by an installer or a system coordinator plus.

Telephony Application Program Interface (TAPI)

The Telephony Application Program Interface (TAPI) is a standard program interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources elsewhere in the world.

Telnet

Telnet is a service that provides terminal-emulation capabilities for logging into the Enterprise Edge unit from a remote location.

Terminal Endpoint Identifier

A digit used to identify devices which are using an ISDN connection for D-channel packet service.

Terminal equipment (TE)

A generic term for devices that connect to an ISDN network. Examples of ISDN TE are ISDN telephones, computers equipped with ISDN cards and video terminals.

Terminals and Sets

A programming section that lets you assign and change settings that apply to the telephones and other devices connected to the Enterprise Edge Server. Terminals and Sets programming is performed by an installer or a system coordinator.

Time and date

A programming section that lets you manually change time or date.

Token-ring

A token-ring is a network topology and data signaling scheme where a special data packet (called a token) is passed from one station to another along an electrical ring. A transmitting station takes possession of the token, transmits the data, then frees the token after the data has made a complete circuit of the electrical ring.

Tone dial telephone

A push button telephone that emits DTMF tones.

TOS

See Type of Service.

Transfer

A feature that lets you redirect a call to another telephone in your Enterprise Edge system, over a network or outside your system.

Transfer Callback

If a transferred call is not answered after a specific number of rings, the call will return to the telephone that made the transfer. The number of rings is assigned under Feature settings in System programming. Transfer Callback does not apply to calls transferred externally.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A language governing communication among all computers on the Internet.

TCP protocol checks packets of information for errors, submits requests for re-transmission in the event of errors and returns multiple packets of a message into the proper original sequence when the message reaches its destination.

IP dictates how packets are sent out over networks and has a packet addressing method that lets any computer on the Internet forward a packet to any other computer that is a step or more closer to the packet's recipient.

Trunk

The physical connection between the Enterprise Edge system and the outside world using either the public telephone system or a private network.

Trunk Answer

A feature you can use to answer a call on any line that has an active Ringing service Service Mode, even if that line does not appear on your telephone. Trunk Answer is enabled in Services programming.

Trunk Media Bay Module

A computer module which provides access to telecommunications trunks. The Digital Trunk Media Bay Module (EE-DTM) provides the connection between a standard digital PSTN T1 or PRI line and the Enterprise Edge system. The Caller ID Trunk Media Bay Module (EE-CTM) provides the ability to access four analog Caller ID PSTN lines.

Type of Service (TOS)

The TOS field is located in the IP packet header and is used in DiffServ processing.

U

UDP

See User Datagram Protocol.

Unsupervised line

A line for which disconnect supervision is disabled. If an external caller hangs up, the system does not detect the disconnection and does not hang up its line. See Disconnect Supervision.

User Data

User Data is an option in the Set Copy feature. User Data refers to the personal settings that are unique to an individual telephone, and are not programmed for the system. User Data is programmed at each telephone.

These settings, for example, include Personal Speed Dial and the assignment of programmable memory buttons.

User Datagram Protocol (UDP)

The UDP is a protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

Like the Transmission Control Protocol, UDP uses IP to actually transfer a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order.

Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

User Filter

See Restriction filter.

User Preferences

A programming section that lets you assign autodialers, user speed dial codes, display contrast, and other settings to a specific telephone or person. You do not have to program these settings at the person’s telephone. User preferences are assigned in Terminals and Sets programming.

User Speed Dial

Two-digit codes (71-94) can be programmed to dial external telephone numbers. User Speed Dial numbers are programmed for each telephone, and can be used only at the telephone on which they are programmed.

V

Voice Call

A feature you can use to make an announcement or begin a conversation through the speaker of another telephone in the system. The telephone you call will not ring. Instead, the person you call will hear a beep and then your voice. Their telephone will beep periodically to remind them that their microphone is open.

Voice Call deny

A feature that prevents your telephone from receiving Voice Calls.

Voice message center

If you have subscribed to Call Display services you can receive visual Voice Message Waiting Indication, providing your telephone has a display. If you have Voice Message Waiting Indication, you can program the telephone numbers required to access up to five different Voice Message Centers. You can also program which of the five Centers is to be accessed by each specific line.

Voice over IP (VoIP)

Voice over IP (VoIP) is the capability to deliver voice using the Internet Protocol. VoIP is a set of facilities for managing the delivery of voice information using the IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

In addition to IP, VoIP uses the real-time protocol (RTP) to help ensure that packets get delivered in a timely way. Using public networks, it is difficult to guarantee Quality of Service (QoS).

Using VoIP, an enterprise positions a VoIP device at a gateway. The gateway receives packetized voice transmissions from users within the company and then routes them to other parts of its intranet (local area or wide area network) or, using a T-1 or E-1 interface, sends them over the public switched telephone network.

W

Wait for dial tone

A feature that causes of sequence of numbers to pause until dial tone is present on the line before continuing to dial. The Wait for dial tone symbol (,) uses two of the 24 spaces in a dialing sequence. This feature requires a Services or Combo Cartridge.

Web cache

A web cache is a server or collection of servers that store copies of Internet content. The web cache server can be either located on the LAN where the clients it serves are also located, or it can be embedded within the enterprise WAN or at the client's Internet Service Provider (ISP).

Web proxy

A web proxy, or HTTP proxy, is a server that acts on behalf of the requester of pages from an HTTP server and the Internet.

Weighted Fair Queuing (WFQ)

WFQ is a queuing method that allows low volume traffic such as Telnet to be given priority and interactive traffic receives higher priority than batch transfers. Also, high bandwidth usage traffic such as batch file transfer traffic gets equal priority with other high bandwidth use traffic.

Wide Area Network (WAN)

A collection of computers or Enterprise Edge Servers connected or networked to each other over long distances, typically using common carrier facilities.

wireless

See Companion.

Index

Numerics

2-way DID
  PRI 377
  PRI dialing plan example 370
2-way service 370

A

access codes 156, 340
accessing Unified Manager settings, system 41
ACD 27
Adding a user profile 254
administration, web based, setting up 37
Agents 27
alarm
  codes 285
  CSU 299
  messages 149
  short term 300
  telephone 149
Alarm Backup Batch Job 253
Alarm Banner 256
Alarm Browser 256
Alarm Database 253
Alarm Manager 253
alarm manager settings, overview 256
alarm service settings, overview 232
Alarm time 184
allow last number redial
  programming 104
AMIS 26
Answer DNs 98
Answer mode 113, 332
assign
  answer DNs 98
  intercom buttons 94
  line pools 97
  lines 95
Audio Messaging Interchange Specification 26
auto DN, programming 157
Automatic Call Distribution 27
automatic route selection (see call routing)
automatic telephone relocation
  programming 302
auxiliary ringer
  programming 117
  troubleshooting 317

B

back up WAN 59
Background music 148
  troubleshooting 317
Backup and Restore 260, 265
  backing up programming 266
  caution when restoring programming 267
  failed restore 267
bar graph (progress indicator) 266
B-channel selection sequence 75
BRI (Basic Rate Interface) module 378–379
BRI (see also ISDN)
BRU 260

C

Call by Call
  example 346
  PRI limits 168
  programming service selection 168
  routing table 130
  service selection 76
  service selection for PRI 166
call log
  automatic 96
  password 93
  set 96
  space 107
Call Offer 247
Call routing 27
  programming 128
called ID 107
Camp timeout delay 152
CAP (Central Answering Position)
  line assignment 97
  programming 154
card edge loopback test 295
carrier access codes 159
carrier failure alarms 298
CbC routing table example 130
central answering position (see CAP)
change DNS 148
Channel Service Unit (see CSU)
channel, disabling PRI 82
CLASS assignment 106
Class of Service
  dialing restriction 333
  security 333
Class of Service (see COS)

clock source
about 75
master 76
primary reference 75
secondary reference 75
CO fail 78
cold start
definition 267
warning (dialog box) 268
common settings 143
Companion programming
cell
assignment 180
neighbours 181
radio neighbour 181
radios 180
disabling registration 177
enabling registration 177
recommended settings 182
re-evaluation 179
re-evaluation status 179
Companion, troubleshooting 326
compression protocol 50
Configuring an ISDN interface 60
configuring management settings
alarm manager, overview 256
user manager, overview 253
configuring resource settings
LAN 46
WAN backup links
access parameters 66
link parameters 65
overview 63
summary parameters 64
WAN primary links
frame relay parameters 54
line parameters 53
overview 49
performance graphs and tables 58
PPP parameters 57
configuring service settings
alarm service, overview 232
DHCP
LAN 194, 198
overview 192
DNS, overview 199
NetLink manager, overview 229
QoS
overview 220
performance graphs and tables 225
QoS monitor
mean opinion score 227
overview 227
routing, overview 200
SNMP
community list 217
manager list 217
trap community list 217
TAPI Service Provider, overview 232
voice mail, overview 240
voice record, overview 232
voice service 189
VoIP Gateway 189
overview 227
Web cache, overview 228
configuring system settings
fault alarm banner 308
introduction 41
performance graphs and tables 308
connecting to Enterprise Edge, methods for
remote dial-in 66
connections, stand alone 379
Contrast Adjustment 309
coordinated dialing plan 335
copy telephone settings 91
COS (Class of Service)
auto DN 157
calls answered with DISA 157
password 160
auto-answer system 331
line restriction 161
user filter 161
with DISA 335
CSU (Channel Service Unit)
alarms 299
description 79
performance statistics 299
stats 297
CSU (Channel Service Unit) line build 78
customizing call display services 106

D

defaults
dialing restriction 125
directory number lengths 162
remote access packages 110
restrictions 125
set restrictions 105
delay
Camp timeout 152
Delayed Ring Transfer 149
Park timeout 152
Transfer callback 152
Delayed ring transfer 149
Deleting a user profile 255
Deleting an ISDN interface 63
deprovisioning a line 81

destination code
description 129, 131
Destination IP Type 240
device
disabling 281
enabling 281
DHCP service settings
LAN 194, 198
overview 192
diagnostics 269
T1 signal 297
test results, system test log 282
dial tone absent on external lines 311
Dialing plan
2-way DID 370
coordinated 335
PRI 377
PRI routing table 130
private DN length 155
public DN length 155
shared line pools 340
using T1 E&M lines 337
dialing restriction 333
defaults 125
exceptions 126
for remote callers 119
line filter 161
line/set restriction 105
maximum length 126
maximum number 126
remote 334
remote user 119
removing a filter 126
Restriction service 333
restrictions 126
set restrictions 104
user filter 161
wild card character 125, 131
dial-on-demand 231
DID (Direct Inward Dial) trunk 332
Digit Absorb 133
Digit Absorption 133
Digital Trunk Interface (see DTI)
Direct dial digit, programming 150, 153, 157
Direct Inward Access
lines in a network 362
Directed pickup 149
directory numbers
changing 148
coordinated dialing plan 335
length 162
DISA (Direct Inward System Access)
DID, trunk 332
DN 157
private networks 363
remote callers 335
disabling
a device 281
a module 279
disconnect supervision
loop start trunks 331
disconnect timer 74
display unreadable, troubleshooting 309
Disposition 239
Diversion 243
DN hunting (see multi-line hunt)
DNS guidelines 199
DNS service settings, overview 199
DPNSS 1 features 242
DSX1 build 78
DTI (Digital Trunk Interface), trunk 328

E

EE-DTM
clock source 75
LEDs 319
electromagnetic compatibility 17
enabling a module 280
Enbloc dialing 137
Entering the software keycodes 41
Enterprise Edge
administration, web-based, setting up 37
IP addresses, setting up
with a laptop 36
with a PC 36
IP Routing information protocol 201
logging off 40
logging on 37
operational considerations 37
rebooting 40
WAN connections
permanent
frame relay 50
PPP 50
with Meridian M1 over PRI 328
Enterprise Edge Link, troubleshooting 316
Enterprise Edge Operator Manager 26
Enterprise Edge Personal Mailbox Manager 26
Enterprise Edge QoS Routing 28
Enterprise Edge system networking 328

error messages
10.5.2 273
11.12.10 273
11.19.9 273
11.5.2 273
14.17.40 274
14.17.41 274
14.17.68 274
14.4.21 273
14.5.77 274
2.5.4 270
2.5.6 270
2.5.8 270
2.xx.4 270
2.xx.6 270
5.16.68 272
5.4.59 271
5.5.39 271
5.5.40 271
5.5.41 271
5.5.45 271
8.4.2. 272
8.5.3 272
8.8.3 272
9.4.2 272
9.6.4 272
9.6.5 272
9.6.6 272
overview 270
user actions 270
Ethernet
WAN connections
permanent
frame relay 50
PPP 50
evening schedule 143
event messages
maintenance 285
significant 286
system restarts 288
exception (see dialing restriction)
extended superframe 78
external code, programming 157
external lines, access code 157
external paging, troubleshooting 317
extra-dial telephone, programming 140

F

Fast 47
Fast Routing 47
fault alarm banner settings 308
feature
codes, troubleshooting 323
using remotely 331
Feature Settings
access codes 156
Call log space 151
CAP assignment 154
Direct dial 153
Held reminder 149
page 152
page tone 149
Park 150
filtering
criteria 390
ranges 390
filters (see also restriction service) 105, 124
first display 107
Fnvram (backup file name) 265
Fnvram.NEW 265
Fnvram.OLD 265
frame relay 50
frame relay parameters, WAN 54
framing format 78

G

General Settings
Feature Settings 148
Remote Access 160
ground start trunk 329

H

hearing-aid compatibility 17
help, customer support 307
Hold
tones, music, or silence 148
Home Location Code 359
Hospitality services 183
hung lines 311
Hunt Groups
about 170
Adding members 171
Assigning lines 173
Broadcast mode 174
Distribution modes 174
Moving members 172
Programming busy line setting 175
Programming the overflow set 175
Programming the queue time-out 175
Removing members 171
Rotary mode 174
Sequential mode 174
Setting the hunt delay 174
Setting the name 176
Unassigning lines 173
usage metrics 302

I

ICMP counters 275
idle line, search for 116
impedance, setting for line 117
Integrated QoS Routing 28
interdigit timeout 154
interface levels 78
internal CSU 79
internal numbers
  changing 148
  coordinated dialing plan 335
  length 162
Intrusion Capability Level 246
Intrusion Protection Level 246
IP addresses, setting up
  with a laptop 36
  with a PC 36
IP options 239
IP Routing 200
  information protocol 201
ISDN (Integrated Services Digital Network)
  bearer capability 373
  BRI card 378–379
  capabilities 371
  capability packages 382
  capability packages, ordering 380
  clocking 379
  data transmission speed 373
  D-channel packet service 388
  installation programming 383
  layers 372
  network synchronization 379
  ordering service 382
  planning service order 372
  programming sequence 383
  S interface 378
  S reference point 378
  services and features 374
  SPID 387
  standards 380
  T reference point 378
  terminal equipment configuration 378
ISDN Access Parameters 61
ISDN Channel Characteristics 61, 62
ISDN loss plan setting 78
ISDN Overview 371
ISDN PRI
  2-way DID 377
  Dialing Plan 377
ISDN Summary 60

J

JAVA Virtual Machine (JVM) 37

L

LAN performance 49
LAN resource settings 46
LAN, DHCP settings 194, 198
LEDs, EE-DTM 319
Legacy networks, port range settings 225
Licensing 41
line
  assignment 95
  control sets 109
  deprovisioning 81
  pool
    access code 158
    access codes 340
    troubleshooting 324
  PRI, about 329
  programming
    name 109
    telco features 118
    trunk/line data 111
  provisioning 81
  redirection feature 368
  restriction programming 118
  selection, for a direct dial telephone 153
  troubleshooting 310–315
line access 93
line coding 78
line parameters, WAN 53
line pool access code 158
line restriction 333
line/set restriction 105, 333
  user filter 161
link parameters, WAN 65
Link time 153
log
  network evt 284
  space
    number of spaces 107
    programming 107
  system administration 283
  system test 282
logging off of Enterprise Edge 40
logging on to Enterprise Edge 37
logon definitions
  configure 38
  download 38
  login 38
  password 38
  upload 38
Loop avoidance, programming 252
loop start trunk
  remote access from public network 331
loopback test, starting 296

loss package 117
loss/gain settings 117
lunch schedule 143

M

M7100 telephone
  accessing external lines 157
M7324 telephone
  CAP 154
maintenance
  alarm codes 285
  bipolar violations 300
  carrier failure alarms 299
  CSU stats 297
  disabling module/cartridges 279
  enabling the module 280
  event messages 285
  identify device connected to system 280
  network event log 284
  programming
    system administration log 283
  short term alarms 300
  system
    administration log 283
    test log 282
    version 278
Management 253
mean opinion score, QoS monitor 227
Media Bay Modules, clock source 75
Meridian 1 341
message centre, selecting 251
Message Waiting Cancellation 249
Message Waiting Indication 249
Message Waiting Indication, setting 251
Message, sending 150
MIB-II
  counters 274
  variables 274
Modem Link Parameters 65
Modifying a user profile 254
module
  enabling 280
  showing inventory 279
  troubleshooting 325
moving telephones (see automatic telephone relocation)
multi-line hunt 374
  groups 382
music
  license 18
  source 18
MWC 249, 251
MWI 249, 251

N

National ISDN standards 380
NetLink manager settings, overview 229
network
  configuration samples 327–369
  event log 284
  options with Enterprise Edge 327
  private 365
  private systems to Enterprise Edge 328
  public network to Enterprise Edge 328
  security 333
  troubleshooting 321–325
  user problems 321
Network Name Display 163
  Business name 165
  calling party name 164
  connected name 164
  interactions 164
  programming 165
  receiving redirected name 164
Network Routing 28
night schedule 143
No free lines 315
Nortel Networks Technical Solutions Centers 307
Not available 314
Not in service 314
NSI string 250
NT1 (network termination type 1) 380
  stand alone connections 379

O

On hold (see hold)
operational considerations 37
Operator Manager 26
optional equipment, troubleshooting 315–317
outbound traffic filter, creating 389
Outgoing Name and Number Blocking 188
Outgoing name and number blocking 165
overflow routing 142

P

packet filtering
  features
    destination address 239
    destination mask 239
    destination port 239
    protocol 237, 239
    source address 237, 239
    source mask 237, 239
    source port 239
Paging, remote 332

parameters
obtaining required values 35
required values 35
Park
retrieving calls 156
timeout delay 152
park prefix 156
password
calls answered with DISA 157
COS 160
using DISA 335
payload loopback test 294
performance 269
performance graphs and tables
QoS 225
system 308
WAN 58
Personal Mailbox Manager 26
Point to Point Protocol (PPP) 50
port range settings
Legacy networks, overview 225
port ranges
QoS, adding 226
QoS, deleting 226
QoS, modifying 226
portable telephone
disabling 177
enabling 177
troubleshooting 326
PPP parameters, WAN 57
PRI (Primary Rate Interface)
trunk 329
PRI channel, disabling 82
PRI dialing plan, 2-way DID 370
PRI line
provisioning 81
PRI line pools 169
PRI line, provisioning 81
PRI Networking
additional configuration 345
Call-by-call services example 346
Meridian 1 341
Meridian M1 configuration 345
primary WAN 59
primary WAN connection 230
prime telephone 149
Private Access Code 359
private line 112
private network 327
remote access 331
sample configurations 365–369
tie lines 363
programming
alarm telephone 149
allow last number redial 104
auto DN 157
backing up 266
call routing 128
CAP assignment 154
features on a set 107, 141
General Settings 147–169
ISDN 383
least cost routing 136
line access 93
lines 108–121
maintenance 259–301
Media Bay Modules 69
on lines
dialing restrictions 141
ISDN (BRI) lines 385
ISDN (PRI) lines 385
trunk/line data programming 111
voice message center 188
services 124–143
system 163
system features
auxiliary ringer 141
called ID 107
CLASS assignment 106
DN length 162
extra-dial telephone 140
log space 107
remote restrictions 119
restriction service 103–106, 124, 141
ringing 139
ringing group 141
schedule times 143
services 143
System Speed Dial 145
telco features 103, 118
trunk answer 139, 140
voice message center 188
system speed dial 145
Telco Features 187
Terminals&Sets 90–107
Programming PRI routing table 130
protocols, routing information 201
provisioning, T1 lines 81
public line 112
public network 327, 362–364

Q

QoS best effort queue counters 277
QoS best effort traffic counters 277
QoS dropped packets counter 277
QoS graph counters 277

QoS module
relationship with the VoIP QoS monitor, overview 220
restrictions and defaults 221
QoS monitor settings
mean opinion score 227
overview 227
QoS port ranges
adding 226
deleting 226
modifying 226
QoS service settings 220
performance graphs and tables 225
QoS session counters 277
Quick 240

R

radio-frequency interference 16, 20
reallocating log space 151
rebooting Enterprise Edge 40
Received number length 162
receiver volume 149
re-evaluation, see Companion programming
registration
information for telephone company 18
on a portable 181
remote
filters 161
system access 330–332
users, troubleshooting 321–325
remote access
COS password 160
defaults 110
dialing restriction 333
DID trunks 332
from public network 331
loop start trunks 331
on a private network 331
PRI trunk 332
restricting 160
security 333
T1 E&M trunks 331
remote dial-in, guidelines 66
Remote Paging 332
remote restriction 334
remote routers, setting up 389
remote system access 330
restore 262, 267
restricting
feature use (see Set Lock)
line at telephone 105
lines 118
remote access 160
remote callers 119
telephones 104, 124
restriction
default 105
dialing 137
service 103, 118, 124, 141
line/set 104, 105
programming 141
schedules 104
Restrictions, using 333
retrieving voice messages 187
ringing service
night schedule 140
ring group assignment 139
ringing groups 139
Route
adding a long distance access code 135
dialing plan to route outgoing PRI calls 137
dialing restrictions 137
for least cost routing 136
for local calling 133
for long distance calling 134
routing
destination codes 129
dialing restrictions 137
sample for local calling 133
sample for long distance calling 134
settings 200
routing, IP
information protocol 201
managing information 200
Routing, network 28
Rule 239
Rule Name 239

S

S interface 378
S or T reference point 378
S reference point 378
Schedule 4 143
Schedule 5 143
Schedule 6 143
schedule names 143
security 333
Class of Service 333
dialing restriction 333
services
evening 143
example of alternate call ringing 139
lunch 143
night 143

programming
common settings 143
restriction services 141
ringing groups 139
ringing service 139
programming ringing sets 141
Schedule 4 143
Schedule 5 143
Schedule 6 143
schedule names 143
schedule times 143
types 138
set
feature and number restrictions 104
restriction
default 105
user filter 161
Setting global WAN parameters 51
setting up
JAVA Virtual Machine 37
logging off of Enterprise Edge 40
logging on to Enterprise Edge 37
operational considerations 37
rebooting Enterprise Edge 40
web-based administration 37
significant event messages 286
SNMP guidelines 216
SNMP service settings
community list 217
manager list 217
trap community list 217
SNMP Trap 253
Software
Integrated QoS Routing 28
Personal Mailbox Manager 26
Unified Messaging 26
Source IP Type 239
Source Routing 239
speed dial 145
Speed Dial programming 145
start and stop times, services 143
Stateful 239
Static DID 370
Static routes 202
Station Set Test 309
statistics 269
Stop restore (dialog box) description 268
summary parameters, WAN 64
superframe 78
support 307
system
administration log 283
processor software 278
sample configurations 327–369
speed dial 145
test log 282, 285, 289
version 278
System Identification Number 41
system performance graphs and tables 308
system settings
Answer key 151
configuring 41

T

T reference point 378
T1
signal diagnostics 297
transmission performance 297
T1 parameters
CO fail 78
CSU line build 78
DSX1 build 78
Framing 78
Line coding 78
target lines
description 329
numbering 329
TCP counters 276
TE (see ISDN terminal equipment)
technical support 307
telephone
control sets 92
direc dial 157
log calls automatically 96
troubleshooting 309
voice message waiting indication 96
Terminals&Sets 90–107
capabilities 98
allow redirect 99
auxiliary ringer 99
direct-dial 99
DND on busy 99
handsfree 99
handsfree answerback 99
hotline 100
page zone 99
paging 99
pickup group 99
priority call 99
redirect ring 99
line access 93
answer DNs 98
intercom keys 94
line assignment 95
line pool access 97
name 91
restrictions 103

telco features 103
user preferences 102
testing
loopback tests 294
system test log 282
Three Party Service 243
tie lines 363
timers, disconnect 74
Tools 265
Transfer callback 152
troubleshooting 305
auxiliary ringer 316
background music 317
Enterprise Edge Link 316
external paging 317
line pools 324
lines 310
modules 318–320
network or remote users 321–325
optional equipment 315–317
portable telephone 326
T1 signal 320
trunk module 320
trunk modules 318
types of problems 306
trunk
answer, programming 140
DTI 328
ground start 329
module, troubleshooting 318, 320
numbering 328
PRI 329
types 328
trunk/line data 111

U

UDP counters 276
Unified Messaging 26
Usage metrics, Hunt groups 302
User Manager 253
user manager settings, overview 253
User Profile 253
utilities, overview 269

V

V.90 modem interface 64
voice mail settings, overview 240
voice message
accessing 96
external center 187
waiting indication 96
Voice Profile for Internet Mail 26
voice record, service settings 232
voice service settings 189
VOIP 115
VoIP Gateway 60
VoIP gateway settings
local gateway 189
overview 227
remote gateway 189
VoIP QoS Monitor
relationship with the QoS module, overview 220
VPIM 26

W

WAN connections
permanent
frame relay 50
PPP 50
WAN Overview 49
WAN resource settings
backup links
access parameters 66
link parameters 65
overview 63
summary parameters 64
primary links
frame relay parameters 54
line parameters 53
overview 49
performance graphs and tables 58
PPP parameters 57
warm start, definition 267
Web cache settings, overview 228
web caching/proxy, guidelines 228
web-based administration, setting up 37
wild card character 125, 131
wiring, loopback test 294